

mitp

Mike
Meyers

10. Auflage

Aktuell zu 220-1001
und 220-1002

CompTIA® A+

Prüfungsvorbereitung ALL IN ONE

Das umfassende Praxis-Handbuch
für IT-Administration, Netzwerktechnik und Support



Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)

Der Verlag räumt Ihnen mit dem Kauf des ebooks das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung und Verarbeitung in elektronischen Systemen.

Der Verlag schützt seine ebooks vor Missbrauch des Urheberrechts durch ein digitales Rechtemanagement. Bei Kauf im Webshop des Verlages werden die ebooks mit einem nicht sichtbaren digitalen Wasserzeichen individuell pro Nutzer signiert.

Bei Kauf in anderen ebook-Webshops erfolgt die Signatur durch die Shopbetreiber. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.


Neuerscheinungen, Praxistipps, Gratiskapitel,
Einblicke in den Verlagsalltag –
gibt es alles bei uns auf Instagram und Facebook
instagram.com/mitp_verlag
facebook.com/mitp.verlag

Für meinen Enkel William Siegmund Kelly.
Ich kann es kaum erwarten,
zusammen mit dir unseren ersten Rechner zusammenzubauen!

Mike Meyers

CompTIA A+

Prüfungsvorbereitung ALL IN ONE

Das umfassende Praxis-Handbuch für IT-Administration, Netzwerktechnik und Support

Aktuell zu den neuen A+-Prüfungen 220-1001 und 220-1002

Übersetzung aus dem Amerikanischen von Knut Lorenzen



mitp

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7475-0100-9
10. Auflage 2020

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Übersetzung der amerikanischen Originalausgabe
Mike Meyers: CompTIA A+® Certification All-In-One Exam Guide, Tenth Edition
(Exams 220-1001 & 220-1002), ISBN 978-1-260-45403-1

Lektorat: Sabine Schulz, Janina Bahlmann
Sprachkorrektorat: Petra Heubach-Erdmann
Coverbild: © pixelnest – stock.adobe.com
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Einleitung

In den Jahrzehnten seit der Vorstellung des IBM Personal Computers (PC) im Jahr 1981 hat sich die Computerwelt drastisch verändert. Gleiches gilt für die Aufgaben der Menschen, die PCs zusammenbauen, warten und auftretende Fehler beheben. Viele Jahre lang kümmerte man sich als PC-Techniker um IBM-kompatible Desktoprechner, auf denen ein Betriebssystem (*Operating System* oder kurz OS) von Microsoft lief, beispielsweise DOS oder später Windows. Abbildung 1 zeigt ein typisches System dieser Zeit, auf dem Microsoft Windows 3.1 läuft. Zur Wartung solch eines Systems benötigte ein Techniker lediglich einen Kreuzschlitzschraubendreher sowie Kenntnisse über die Hardware und das Betriebssystem.



Abb. 1: Ein IBM-kompatibler PC, circa 1989

Heutzutage besteht die Computerlandschaft aus einer Unzahl von Geräten aller möglicher Form und Größe, die den unterschiedlichsten Zwecken dienen. Wie viele computerartige Geräte benutzen Sie jeden Tag? Ernsthaft: Zählen Sie mal nach!

Ich beschreibe nun, welche Geräte ich persönlich jeden Tag so verwende. Morgens werde ich durch den Alarm meines Smartphones aufgeweckt. Ich nutze einen Rechner mit Windows oder macOS, der sich über das Internet mit anderen Computern verbindet, um Nachrichten zu lesen und E-Mails abzurufen. Falls beide Rechner schon von anderen Familienmitgliedern belegt sind, greife ich auf einen Laptop zurück, auf dem Ubuntu Linux läuft, um diese Aufgaben zu erledigen. Im Fitnessstudio überwacht eine Smartwatch meine Übungen und meinen Puls. Auf dem Weg zur Arbeit erledigt der Computer in meinem Auto die Navigation und versorgt mich mit Verkehrsmeldungen. Im Büro bin ich buchstäblich von Dutzenden Computern umzingelt, denn wirklich jeder benutzt entweder einen Desktop, einen Laptop, ein Tablet oder ein Smartphone sowie weitere tragbare Geräte – siehe Abbildung 2.

Irgendjemand muss all diese Geräte aufbauen, warten, überprüfen und reparieren. Und da Sie dieses Buch lesen, nehme ich doch an, dass *Sie* dieser Jemand sind. Als moderner *PC-Techniker* müssen Sie eine Menge über all diese Systeme wissen, und daher werden Sie mit vielen verschiedenen Geräten in Berührung kommen, auf denen ebenso viele unterschiedliche Systeme laufen. Außerdem sind fast alle diese Geräte untereinander verbunden – und das zu ermöglichen, gehört ebenfalls zu den Aufgaben des PC-Technikers.



Abb. 2: Lauter Computer!

Hinweis

In diesem Buch werden der Begriff »Personal Computer« und die Abkürzung »PC« ganz allgemein zur Bezeichnung von computerartigen Geräten verwendet. Mit »PCs« sind stets Geräte gemeint, die von Technikern bedient, eingerichtet und repariert werden.

Sie finden in diesem Buch alles, was Sie wissen müssen, um ein hervorragender PC-Techniker zu werden. Auf den ersten Blick scheint es sich um eine riesige Informationsmenge zu handeln, aber ich werde erläutern, wie all diese Systeme arbeiten und miteinander kommunizieren und Sie werden schon bald die Muster erkennen, die den Funktionsweisen zugrunde liegen. Bei der Lektüre des Buchs und der Arbeit mit Computern nimmt das Ganze irgendwann plötzlich Gestalt an – Sie werden sehen!

Auf dem Weg dorthin werden Sie Bescheinigungen erlangen, mit denen Sie Ihre Kenntnisse Arbeitgebern und Kunden gegenüber nachweisen können. Der verbleibende Teil dieses Kapitels erläutert die zur Erlangung dieser Zertifizierung erforderlichen Schritte.

Das CompTIA A+-Zertifikat

In fast allen Berufen gibt es Kriterien, die Sie erfüllen müssen, um Ihre Kompetenz und Eignung nachzuweisen. Diese unterscheiden sich von Beruf zu Beruf zwar sehr, aber früher oder später müssen Sie Tests oder Prüfungen absolvieren. Durch das Bestehen dieser Prüfungen können Sie nachweisen, dass Sie über die für Ihren Beruf erforderlichen Fähigkeiten verfügen, egal ob Sie ehrgeiziger Installateur, Lehrer, Frisör oder Rechtsanwalt sind.

Wenn Sie die Prüfungen erfolgreich bestehen, dann erhalten Sie von den durchführenden Organisationen ein *Zertifikat*, also ein Zeugnis, eine Mitgliedsnummer oder einen Mitgliedsausweis. Solche Befähigungsnachweise bzw. Zertifizierungen geben potenziellen Kunden und Arbeitgebern die Bestätigung, dass Sie auch wirklich können, was Sie zu können behaupten! Ohne diese Nachweise würden Sie in diesem Beruf entweder nicht arbeiten oder kaum jemanden finden, der Ihnen das notwendige Vertrauen schenkt.

Moderne PC-Techniker erlangen das CompTIA A+-Zertifikat, die grundlegende Bescheinigung, die Kompetenz in der Informationstechnologie (IT) nachweist. Soll heißen: Kenntnisse der Computertechnologie und aller anderen Dinge, die notwendig sind, um Computer miteinander zu vernetzen und zu warten.

Das *CompTIA A+-Zertifikat* ist ein industrieweit und herstellerneutral entwickeltes Zertifizierungsprogramm, das von der CompTIA (*Computing Technology Industry Association*) entwickelt und gesponsert wird. Sie erhalten dieses Zertifikat, indem Sie zwei Prüfungen absolvieren, die am PC stattfinden und auf dem Multiple-Choice-Verfahren basieren. Diese Prüfungen decken ab, was Techniker nach zwölf Monaten praktischer Arbeit mit PCs (als Angestellte oder als studentische Hilfskräfte) wissen sollten. Das CompTIA A+-Zertifikat erfreut sich einer breiten Anerkennung in der Computerindustrie. Bis heute haben mehr als 1.000.000 PC-Spezialisten ein CompTIA A+-Zertifikat erhalten und es damit zu dem am weitesten verbreiteten IT-Zertifikat gemacht.

Wer ist die CompTIA?

Die CompTIA ist ein gemeinnütziger Industriefachverband mit Hauptsitz in Oakbrook Terrace (Illinois). Er hat mehr als 20.000 Mitglieder in 102 Ländern. Sie finden CompTIA-Niederlassungen an Standorten wie Düsseldorf, London, Amsterdam, Dubai, Johannesburg, Tokio und São Paulo.

Die CompTIA versteht sich als ein Forum für die Vernetzung und die Zusammenarbeit der Mitglieder. Sie repräsentiert ihre Mitglieder gegenüber Behörden und bietet Zertifizierungen für viele verschiedene Bereiche der Computerindustrie an. CompTIA sponsert CompTIA A+-, CompTIA Network+-, CompTIA Security+- und andere Zertifikate. CompTIA verfolgt laufend die Entwicklungen in der IT-Industrie und prüft fortwährend die Möglichkeit neuer Zertifikate, die wegen der sich stetig ändernden Anforderungen der Mitgliederbasis erforderlich werden. Einzelheiten über andere Zertifikate, die Sie von CompTIA erhalten können, erfahren Sie über die CompTIA-Websites unter `www.comptia.org` und `www.comptia.de`.

CompTIA bietet CompTIA A+-Zertifikate seit 1993 an. Als dieses Zertifikat debütierte, wurde es von der IT-Industrie zunächst weitgehend ignoriert. Nach diesen Anfangsschwierigkeiten ist die CompTIA A+-Zertifizierung jedoch mittlerweile zur De-facto-Voraussetzung und einer Eintrittskarte im PC-Bereich geworden. Viele Unternehmen erwarten von ihren technischen Mitarbeitern eine CompTIA A+-Zertifizierung, während das CompTIA A+-Zertifikat selbst in den USA und international weitreichende Anerkennung findet.

Der Weg zu anderen Zertifizierungen

Die meisten großen und kleinen IT-Unternehmen betrachten die CompTIA A+-Zertifizierung als Grundvoraussetzung für eine Beschäftigung im IT-Bereich. Was darauf folgt, hängt von vielen Faktoren ab, etwa von Ihren Interessen und den Anforderungen Ihres Unternehmens. Wir betrachten zunächst verschiedene Zertifizierungsoptionen der CompTIA und anschließend die herstellerspezifischen Zertifizierungen von Microsoft und Cisco.

CompTIA Core-Zertifizierungen

CompTIA A+ ist Teil der CompTIA Core-Zertifizierungen. Viele Techniker erwerben nach der A+-Zertifizierung weitere Core-Zertifizierungen, bevor sie sich spezialisieren. Dabei handelt es sich um vier Zertifizierungen:

- CompTIA IT Fundamentals (ITF+)
- CompTIA A+ (1001 heißt *Core 1* und 1002 *Core 2*)
- CompTIA Network+-Zertifizierung
- CompTIA Security+-Zertifizierung

Die CompTIA bezeichnet die A+-Prüfungen als die Core-Reihe (Core 1 und Core 2).

CompTIA ITF+ deckt die Grundlagen der Computernutzung ab, die heutzutage jeder kennen muss. Dazu gehören Kenntnisse über verschiedene Computertypen, die Fähigkeiten von Computern, die Funktionsweise von Netzwerken und Grundlagen der Sicherheit. Wenn Sie bereits eine A+-Zertifizierung besitzen, brauchen Sie die ITF+-Zertifizierung nicht. Sie ist allerdings für Neulinge empfehlenswert, weil sie viele Wissenslücken schließt.

CompTIA Network+ fährt damit fort, womit Sie in den Teilen der A+-Zertifizierungen angefangen haben, die sich mit Netzwerken befassen. Wir leben in einer vernetzten Welt. Techniker müssen Netzwerke von Grund auf verstehen, um die in größeren Unternehmensnetzwerken anfallenden Aufgaben erledigen zu können. Die Network+-Zertifizierung bescheinigt Ihnen Ihre Fähigkeiten als Netzwerktechniker, einschließlich Kenntnisse der Netzwerk-Hardware, der Infrastruktur, der Installation und der Fehlerbehebung. Die Network+-Zertifizierung ist nach der A+-Zertifizierung der folgerichtige nächste Schritt.

Auf ähnliche Weise ergänzt die CompTIA Security+-Zertifizierung die A+- und Network+-Zertifizierung, geht aber sehr viel ausführlicher darauf ein, wie man Netzwerke vor Angriffen schützt, und vermittelt die Richtlinien, an die sich jedes sicherheitsbewusste Unternehmen halten sollte. Ich empfehle, die Security+-Zertifizierung nach der Network+-Zertifizierung zu erwerben. Dadurch werden Ihre Kenntnisse als Techniker in einem großen Unternehmen abgerundet.

Spezielle CompTIA-Zertifizierungen

Die CompTIA bietet verschiedene weiterführende Zertifizierungen an, die auf den Core-Zertifizierungen aufbauen. Diese sind entweder auf ein IT-Fachgebiet spezialisiert oder vermitteln besondere Fähigkeiten in bestimmten Bereichen, wie Infrastruktur, Cybersicherheit oder Fachkompetenz.

Hinweis

Weitere Informationen über die Wege, die man bei den CompTIA-Zertifizierungen einschlagen kann, finden Sie unter `https://certification.comptia.org/certifications/which-certification`.

Bei der Infrastruktur geht es um die Rechner und Betriebssysteme, die Unternehmensorganisationen am Leben erhalten. In dieser Reihe gibt es drei Zertifizierungen:

- CompTIA Linux+
- CompTIA Server+
- CompTIA Cloud+

Viele große Unternehmen setzen auf Linux-Server, um eine Vielzahl von Aufgaben zu erledigen. Zum Betreiben der Server und der Server-Infrastruktur sind spezielle Kenntnisse erforderlich. Da weite Teile der Branche Cloud-basiertes Computing nutzen, wird es für IT-Fachleute immer wichtiger, zu wissen, wie man es in einem Unternehmen erfolgreich einsetzt.

Bei der Cybersicherheit geht es um die Schwarze Kunst der Netzwerksicherheit – wie man sich vor bösen Buben schützt, nicht wie man selbst zu einem genialen Bösewicht wird. Hier gibt es drei Zertifizierungen:

- CySA+
- Pentest+
- CASP+

Diese Zertifizierungen belegen, dass Sie die Fähigkeit besitzen, Netzwerke jeglicher Größe zu analysieren, Schwachstellen aufzuspüren und Netzwerke außerordentlich gut zu schützen. Hier können Sie die in den Core-Zertifizierungen erworbenen Kenntnisse anwenden und diese als Grundlage dafür nutzen, zu einem Sicherheits-Guru zu werden.

In der Reihe *Fachkompetenz* gibt es ebenfalls drei Zertifizierungen, die darauf abzielen, Ihre Fähigkeiten im alltäglichen Umgang mit Informationstechnologien zu verbessern:

- Project+
- Cloud Essentials
- CTT+

Projektmanagement ist bei der Umsetzung umfassender IT-Projekte von großer Bedeutung. Projektmanager belegen durch diese Zertifizierungen ihre Fähigkeiten. Bei den Cloud Essentials geht es darum, was Sie – als Geschäftsmann, nicht als IT-Held – über Cloud-Computing wissen müssen. CTT+ schließlich ist für Leute wie mich, denn das Zertifikat belegt, dass man weiß, wie man Erwachsenen IT-Kompetenz vermittelt.

Nach den Core-Zertifizierungen liegt es nicht auf der Hand, welchen Weg man hinsichtlich weiterer Zertifizierungen einschlagen sollte, das ist vielmehr situationsbedingt. Wenn Sie beispielsweise feststellen, dass die Fähigkeiten eines Projektmanagers für Sie und Ihr Unternehmen von großem Nutzen wären, ergibt die Project+-Zertifizierung durchaus Sinn.

Microsoft-Zertifizierung

Die Betriebssysteme von Microsoft sind Schaltzentrale eines Großteils aller installierten Netzwerke. Für diese Netzwerke braucht man qualifiziertes Support-Personal, damit sie optimal laufen. Die verschiedenen Microsoft-Zertifizierungen für Netzwerkprofis sind der natürliche nächste Schritt nach den CompTIA-Zertifizierungen. Damit sind unterschiedlichste Laufbahnen und Prüfungen möglich, die vom einfachen Windows-10-Experten bis hin zu zahlreichen MCSE-Zertifizierungen (*Microsoft Certified Solution Experts*) und darüber hinaus reichen. Über Einzelheiten der Microsoft-Angebote können Sie sich auf der Website `www.microsoft.com/learning` informieren.

Cisco-Zertifizierung

Die Router der Firma Cisco sorgen überwiegend dafür, dass nicht nur das Internet, sondern auch die meisten Intranets auf der ganzen Welt funktionieren. Ein *Router* ist ein Netzwerkgerät, das den Informationsfluss über Netzwerke steuert und leitet, wie beispielsweise E-Mail-Nachrichten, Surfen im Internet usw. Cisco bietet IT-Zertifizierungen auf verschiedenen Ebenen an, mit denen die Fähigkeit zum Umgang mit Cisco-Produkten belegt werden kann, wie z.B. die CCNA-Zertifizierung (Cisco Certified Network Associate) und zahlreiche weitere spezialisiertere Zertifizierungen. Weitere Einzelheiten erfahren Sie z.B. auf der Cisco-Website unter der Adresse `www.cisco.com/web/learning/certifications`.

CompTIA A+-Lernziele

Die CompTIA unterteilt die A+-Zertifizierung in zwei Prüfungen: *CompTIA A+ 220-1001* und *CompTIA A+ 220-1002* genannt. Es ist außerdem üblich, diese beiden Prüfungen als die 2019-Prüfungen zu bezeichnen, allerdings nennt die CompTIA sie jetzt auch Core 1 und Core 2.

Auch wenn Sie die Prüfungen in beliebiger Reihenfolge ablegen können, empfehle ich doch, erst die Prüfung 220-1001 und dann die Prüfung 220-1002 anzustreben. Die Prüfung 220-1001 konzentriert sich auf Begriffe und Technologien, grundlegende Aufgaben wie das Aufrüsten des Arbeitsspeichers und elementaren Support für Netzwerke und mobile Geräte. Die Prüfung 220-1002 baut auf der Prüfung 220-1001 auf und konzentriert sich auf Betriebssystem-Support, fortgeschrittene Konfigurationsaufgaben und Fehlerbehebungen.

Die beiden Prüfungen sind ausgesprochen praktisch orientiert und legen, außer bei der Fehlerbehebung, nur geringen oder keinen Wert auf theoretische Aspekte. Alle Fragen folgen entweder dem Multiple-Choice-Schema oder fordern Sie dazu auf, den richtigen Teil einer Abbildung anzuklicken. Es folgt ein Beispiel des Fragetyps, dem Sie in den Prüfungen begegnen werden:

Ein Laserdrucker druckt nur leere Seiten. Was sollten Sie als Erstes überprüfen?

A. Druckertreiber

B. Tonerkartusche

C. Druckereinstellungen

D. Papierzufuhr

Die richtige Antwort ist B, die Tonerkartusche. Zwar gibt es auch Argumente für die anderen Antworten, jedoch sagt Ihnen der gesunde Menschenverstand (und Ihre Befähigung als PC-Techniker), zunächst einmal das auf der Hand Liegende zu überprüfen.

Bei den Prüfungen des Jahres 2019 kommt ein einheitliches Format zum Einsatz. Den Teilnehmern wird eine Reihe von Fragen vorgelegt und die erreichte Punktzahl richtet sich nach der Anzahl der richtig beantworteten Fragen. Die CompTIA nimmt gelegentlich Änderungen vor, daher sollten Sie sich auf der CompTIA-Website informieren, bevor Sie mit den Prüfungsvorbereitungen beginnen. Die Prüfungen bestehen aus jeweils etwa 90 bis 100 Fragen.

Beachten Sie, dass CompTIA den Prüfungen jederzeit neue Fragen hinzufügen kann, um den Inhalt jeweils aktuell zu halten. Die Themen der Prüfungen werden sich zwar nicht ändern, aber es werden von Zeit zu Zeit je nach Bedarf neue Fragen hinzukommen. Bei dieser neuen Vorgehensweise wird es zunehmend wichtig, Konzepte verstanden zu haben und über ein solides technisches Wissen aus dem PC-Bereich zu verfügen, anstatt bestimmte Fragen und Antworten, die in früheren Tests möglicherweise bereits vorgekommen sind, auswendig zu lernen. Kein Buch und keine Quelle im Internet wird alle richtigen Antworten bereitstellen können, da sich die Fragen laufend ändern. In dieser Hinsicht haben Sie aber Glück gehabt, denn dieses Buch bringt Ihnen nicht nur die einzelnen Maßnahmen bei, die Sie in bestimmten Fällen ergreifen können, sondern soll Ihnen auch vermitteln, *warum* Sie bestimmte Maßnahmen ergreifen. Bei neuen Problemen (oder Prüfungsfragen) können Sie dann auf die richtigen Lösungen bzw. Antworten schließen. Und dann lassen sich nicht nur die Prüfungen leichter bestehen, sondern Sie werden auch zu einem besseren PC-Techniker!

Auf der englischsprachigen Website `www.totalsem.com/100x` finden Sie verschiedene Übungsaufgaben und Zusatzinformationen zum Buch. Wenn es zu einem Thema eine passende Übung gibt, wird an der entsprechenden Stelle darauf verwiesen.

Vornehmlich Windows

Die CompTIA A+-Prüfungen befassen sich mit sechs verschiedenen Betriebssystemen und innerhalb der Betriebssysteme mit vielen unterschiedlichen Versionen. Wenn Sie sich die nachfolgend aufgeführten Lernziele ansehen, werden Sie allerdings feststellen, dass sich der größte Teil der Fragen auf das Betriebssystem Microsoft Windows bezieht, wie es auf Arbeitsstationen oder am heimischen Arbeitsplatz zu finden ist. Die Fragen decken auch einen bestimmten und begrenzten Bereich der Betriebssysteme macOS, Linux, Chrome OS, iOS und Android ab. Es könnten sogar Fragen zu Windows Phone vorkommen.

Die Lernziele der beiden Prüfungen beziehen sich auf die folgenden Betriebssysteme:

- Windows 7 Starter, Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, Windows 7 Enterprise
- Windows 8, Windows 8 Pro, Windows 8 Enterprise
- Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise
- Windows 10 Home, Windows 10 Pro, Windows 10 Enterprise
- macOS
- Linux
- Chrome OS
- iOS
- Android

Tipp: Empfehlen eines Betriebssystems

Stellen Sie sich die folgende Situation vor: Eine Ihrer ersten Kundinnen möchte ihre Computerausstattung verbessern, ist aber ratlos. Sie sollen ihr etwas empfehlen. Auf diese Weise können Sie am Anfang Ihres Weges zur CompTIA A+-Zertifizierung sehr gut lernen, Ihre schon vorhandenen Kenntnisse einzuschätzen.

Öffnen Sie auf Ihrem Computer oder Smartphone einen Webbrowser und besuchen Sie den von mir bevorzugten Onlinehändler für Technikprodukte (`www.newegg.com`) und durchforsten Sie die angebotenen Computersysteme. Welches Betriebssystem kommt am häufigsten vor? Was können Sie den Vergleichstests zwischen beispielsweise Chrome OS und Windows 10 entnehmen? Werden dort auch Apple-Produkte angeboten?

Wenden Sie aber nicht allzu viel Zeit für diese Übung auf. Sie dient lediglich dazu, Sie allmählich an die typische Vorgehensweise zu gewöhnen, die wir Techniker nutzen, um auf dem Laufenden zu bleiben. Ich komme in den nachfolgenden Kapiteln auf diese Übung zurück, damit Sie im Laufe der Zeit Ihren Wissensstand und die Zufriedenheit damit abschätzen können.

Prüfung 220-1001

Die Fragen der CompTIA A+-Prüfung 220-1001 gehören zu fünf verschiedenen Wissensgebieten. Die Anzahl der Fragen aus jedem Bereich richtet sich nach den in Tabelle 1 angegebenen Prozentwerten.

Wissensgebiet	Prozentuale Gewichtung
1.0 Mobile Geräte	14%
2.0 Netzwerke	20%
3.0 Hardware	27%
4.0 Virtualisierung und Cloud-Computing	12%
5.0 Fehlerbehebung (Hardware/Netzwerk)	27%

Tabelle 1: Wissensgebiete und deren Gewichtung in der Prüfung 220-1001

Die Prüfung 220-1001 testet Ihr Wissen über Computerkomponenten und erwartet von Ihnen, dass Sie praktisch alle im PC-Bereich gängigen Gerätetypen und deren Varianten identifizieren können. Nachfolgend eine Liste:

- Festplatten
- Optische Laufwerke
- Solid-State-Laufwerke
- Mainboards
- Netzteile
- CPUs
- RAM
- Bildschirme
- Eingabegeräte (z.B. Tastatur, Maus und Touchscreen)
- Grafik- und Multimediakarten
- Netzwerk- und Modemkarten
- Kabel und Stecker
- Kühlkörper, Lüfter und Flüssigkühlsysteme
- Laptops und mobile Geräte

- Drucker und Multifunktionsgeräte
- Scanner
- Netzwerk-Switches, Verkabelung und WLAN-Adapter
- Biometrische Geräte
- Virtualisierung
- Cloud-Computing

Die Prüfung 220-1001 testet Ihre Fähigkeit, die gesamte für einen PC erforderliche Hardware zu installieren, zu konfigurieren und zu warten. Sie müssen beispielsweise eine Festplatte installieren und einrichten oder Geräte unter Windows 7, Windows 8, Windows 8.1 und Windows 10 konfigurieren können. Sie müssen außerdem verstehen, was Gerätetreiber sind.

Die Prüfung 220-1001 prüft auch Ihr Wissen über mobile Geräte. Der Smartphone- und Tablet-Markt umfasst zwar ein unglaublich breites Spektrum an Hard- und Software, die Prüfung 220-1001 konzentriert sich allerdings auf Apples iOS und Googles Android (allerdings könnte auch eine Frage zu Chrome OS oder Windows Phone vorkommen). Sie müssen sowohl mit der Hardware als auch mit der Software umgehen können.

Die Prüfung 220-1001 testet auch ausführlich Netzwerkkenntnisse. Sie müssen beispielsweise wissen, wie ein lokales Netzwerk (*Local Area Network*, LAN) eingerichtet wird und Verkabelungsstandards, Netzwerkprotokolle und die Konfigurationsmöglichkeiten in Windows kennen.

In der Prüfung 220-1001 werden Fragen zum Cloud-Computing und zu Virtualisierungstechnologien gestellt. Sie müssen Cloud-Dienste wie Cloud-Speicher und nur per Internet verfügbare Anwendungen kennen. Sie werden auch gefragt, wie man virtuelle Maschinen in einer Netzwerkumgebung einrichtet und wartet.

Für die Prüfung 220-1001 müssen Sie eine Menge über die Fehlerbehebung bei Störungen der Hardware und des Netzwerks wissen. So werden Ihnen z.B. Fragen zur Fehlerbehebung bei einem Ausfall des Netzwerks gestellt.

Prüfung 220-1002

Die CompTIA A+-Prüfung 220-1002 deckt vier Wissensgebiete ab. In Tabelle 2 sind die prozentualen Anteile der Fragen zu den verschiedenen Wissensgebieten aufgeführt.

Wissensgebiet	Prozentuale Gewichtung
1.0 Betriebssysteme	27%
2.0 Sicherheit	24%
3.0 Fehlerbehebung (Software)	26%
4.0 Betriebsabläufe	23%

Tabelle 2: Wissensgebiete und deren Gewichtung in der Prüfung 220-1002

Die Prüfung 220-1002 umfasst die Konfiguration, Reparatur und Fehlerbehebung von Betriebssystemen – vornehmlich Microsoft Windows, es kommen jedoch auch Fragen zu macOS, verschiedenen Linux-Distributionen und Google Chrome OS vor. Sie müssen wissen, wie Sie sich in Windows bewegen und die Aufgaben verstehen, die beim Aktualisieren, Aufrüsten und Installieren von Windows 7, Windows 8, Windows 8.1 und Windows 10 anfallen. Sie müssen die Standarddiagnosewerkzeuge von Windows kennen, damit Sie bei der Fehlerbehebung mit spezialisierten Technikern zusammenarbeiten können. Vergewissern Sie sich, dass Sie sich in Windows auskennen, denn bei ungefähr einem Viertel der Fragen der Prüfung 220-1002 handelt es sich um Aufgaben aus diesem Bereich.

Sie müssen wissen, wie die Benutzerschnittstellen von Linux und macOS bedient werden. Darüber hinaus wird geprüft, ob Sie die verschiedenen Werkzeuge zur Wartung korrekt ausführen oder ein

Backup anlegen können und so weiter. Die Prüfung geht bei der Konfiguration von iOS und Android ziemlich in die Tiefe, beispielsweise bei der Einrichtung von E-Mail und der Absicherung der Geräte. Allerdings spielt die Sicherheit nicht nur bei mobilen Geräten eine Rolle ...

Die Sicherheit ist ganz allgemein ein Schwerpunkt der Prüfung 220-1002. Sie müssen auf diesem Gebiet eine ganze Menge wissen: von physischer Sicherheit (Türschlösser, Netzhaut-Scanner) über Kenntnisse der Gefährdung der Sicherheit (Schadsoftware, Viren) bis zu den verschiedenen Möglichkeiten, einen einzelnen Computer abzusichern. Hierzu gehört außerdem Sachverstand beim Recyceln und Entsorgen von Computerschrott.

Sie werden auch nach Methoden zur Absicherung eines Netzwerks gefragt. Sie müssen wissen, wie man auf einen SOHO-Router (*Small Office/Home Office*, Klein- und Heimbüros) oder einen drahtlosen Zugriffspunkt zugreift und wie das Gerät konfiguriert werden muss, um Ihr Netzwerk zu schützen.

Außerdem legt diese Prüfung großen Wert auf Betriebsabläufe, wie etwa Sicherheits- und Umweltschutzaspekte sowie Kommunikation und Professionalität. Sie müssen gefährliche Situationen erkennen und vermeiden. Die Prüfung testet Ihre Fähigkeit, effektiv mit Kunden und Arbeitskollegen zu kommunizieren. Sie müssen professionelles Verhalten vorweisen und zeigen, dass Sie Takt, Diskretion und Respekt vor anderen Menschen und deren Eigentum aufbringen.

Der Weg zur Zertifizierung

Sie erhalten die CompTIA A+-Zertifizierung ganz einfach, indem Sie zwei computergestützte Multiple-Choice-Prüfungen ablegen. Für die Teilnahme an den CompTIA A+-Zertifizierungsprüfungen müssen keine Voraussetzungen erfüllt werden. (Von entsprechenden Computerkenntnissen wird natürlich ausgegangen.) Sie müssen keine vorbereitenden Kurse belegen und keine Trainingsmaterialien kaufen. Sie bezahlen allerdings eine Gebühr für die zwei Prüfungen. Anschließend werden Sie sofort darüber in Kenntnis gesetzt, ob Sie bestanden haben oder durchgefallen sind. Wenn Sie beide Prüfungen bestanden haben, dann sind Sie »CompTIA A+-zertifiziert«.

Um zertifiziert zu bleiben, müssen Sie entweder alle drei Jahre die Prüfung erneut ablegen oder aber gemäß den Vorgaben der CompTIA an regelmäßigen Schulungen teilnehmen.

Die Wiederholung der Prüfung ist leicht verständlich, die Anforderungen einer fortdauernden Weiterbildung sind jedoch etwas komplizierter. Anstatt zu versuchen, das alles an dieser Stelle zu erläutern, verweise ich auf die CompTIA-Unterlagen, die Sie unter `https://certification.comptia.org/continuing-education` finden.

Falls Sie den Weg der fortlaufenden Weiterbildung beschreiten möchten, ist das Wichtigste, dass Sie innerhalb des Zeitraums von drei Jahren 20 CEUs (*Continuing Education Units*) erwerben müssen, um Ihre CompTIA A+-Zertifizierung zu verlängern. Wie verdient man sich diese CEUs? Sie können an Veranstaltungen und Seminaren der Branche teilnehmen, Vorträge halten, IT-Schulungen besuchen, Lehrveranstaltungen abhalten oder eine weitere fortgeschrittene Zertifizierung erlangen. Die Anzahl der CEUs, die Sie für die Durchführung dieser Aufgaben erhalten, ist unterschiedlich hoch. Jede dieser Tätigkeiten muss jedoch der CompTIA zur Überprüfung nachgewiesen werden.

Auswahl eines Prüfungszentrums

Die eigentlichen CompTIA A+-Prüfungsverfahren werden von dem Unternehmen Pearson VUE verwaltet. Es gibt weltweit mehr als 5.000 Prüfungszentren von Pearson VUE in 165 Ländern. Sie können die Prüfungen in jedem dieser Prüfungszentren ablegen. Sie können sich das nächstgelegene Prüfungszentrum aussuchen und Ihre Prüfungen mithilfe Ihres bevorzugten Webbrowsers planen: `www.vue.com`.

Sie müssen die Prüfung bei der Anmeldung bezahlen. Machen Sie sich darauf gefasst, dass die Abwicklung ein wenig dauern kann. Halten Sie beim Anruf neben Ihrem Personalausweis eine Kreditkarte bereit. Natürlich stellt Pearson VUE Ihnen auch eine Rechnung aus, aber Sie können die Prüfung erst ablegen, wenn die Zahlung vollständig erfolgt ist.

Bei speziellen Anforderungen hilft Ihnen Pearson VUE gerne weiter, aber möglicherweise wird dadurch die Auswahl der möglichen Prüfungsorte begrenzt.

Kosten der Prüfung

Die Kosten für die Prüfung sind davon abhängig, ob Sie für ein Mitglied der CompTIA arbeiten oder nicht. Zum Zeitpunkt der Drucklegung dieses Buches betragen die Kosten für Nicht-Mitglieder der CompTIA jeweils knapp 200 Euro für die beiden A+-Prüfungen. Die internationalen Preise variieren, aber Sie können sich auf der Website von CompTIA über die aktuellen Preise informieren. Natürlich können die Preise sich jederzeit ohne Benachrichtigung ändern, lesen Sie also am besten auf der Website von CompTIA nach, um die aktuellen Preise zu erfahren.

Den vollen Preis bezahlt allerdings kaum jemand. Praktisch alle Organisationen, die CompTIA A+-Schulungen und Prüfungen anbieten, haben auch vergünstigte Gutscheine im Angebot, sogenannte *Voucher*. Sie erwerben einen Voucher und nutzen anstelle Ihrer Kreditkarte die Voucher-Nummer, wenn Sie sich zur Prüfung anmelden. Zu jeder Prüfung gehört ein eigener Voucher, das heißt Sie benötigen zwei Voucher, um beide A+-Prüfungen abzulegen. Es ist also für gewöhnlich nicht erforderlich, den vollen Preis für die CompTIA-A+-Prüfungen zu zahlen.

Ablegen der CompTIA A+-Prüfungen

Die A+-Zertifizierung wird von der CompTIA dafür entwickelt, das Wissen eines Technikers zu prüfen, der nur etwa zwölf Monate Erfahrung hat – kein Grund also, sich allzu große Sorgen zu machen! Sie müssen das CAS-Timing zum Übertakten der DDR4-Module im CMOS nicht ändern oder den Unterschied zwischen den Intel- und AMD-Chipsätzen nicht erläutern können. Denken Sie also mehr an praktisches Wissen und Standards: Lesen Sie dieses Buch, prägen Sie sich die grundlegenden Konzepte und Vorgehensweisen ein, bearbeiten Sie die Aufgaben und wiederholen Sie die Themen, die Sie noch nicht beherrschen – dann werden Sie die Prüfungen ohne Probleme bestehen.

Hinweis

Diejenigen unter Ihnen, die mehr über die Verwaltung von PCs und die Fehlerbehebung erfahren wollen, können derselben Vorgehensweise folgen wie diejenigen, die eine Zertifizierung anstreben. Denken Sie praktisch und arbeiten Sie mit dem PC, während Sie die einzelnen Kapitel nachvollziehen.

Einige Leser haben möglicherweise gerade erst die Schule verlassen, die Prüfungsvorbereitung ist also nichts Neues für sie. Falls Ihre Schulzeit und Ihre Prüfungen jedoch schon länger zurückliegen oder wenn Sie denken, Sie könnten ein paar praktische Tipps gebrauchen, dann wird der nächste Abschnitt sehr hilfreich für Sie sein. Er beschreibt eine bewährte Strategie für das Ablegen und Bestehen der CompTIA A+-Prüfungen. Probieren Sie es aus. Es funktioniert.

Nehmen Sie sich selbst in die Pflicht!

Zuallererst sollten Sie sich überlegen, wann der richtige Zeitpunkt für das Ablegen der Prüfung ist. Haben Sie schon einmal gehört, dass Diamanten unter Hitze und Druck entstehen? Das gilt auch für Sie: Wenn Sie zu lange zaudern und zögern und zu wenig Eifer entwickeln, brauchen Sie mehr Zeit, bis Sie sich an die Prüfungen wagen können. Vielleicht verschieben Sie den Termin immer wieder und absolvieren sie zu guter Letzt gar nicht. Tun Sie sich selbst den Gefallen und stellen Sie fest, wie viel Zeit Sie zur Vorbereitung auf die Prüfungen benötigen, und legen Sie dann einen Prüfungstermin fest. Sobald Sie wissen, dass demnächst eine Prüfung ansteht, wird es Ihnen viel leichter fallen, den Fernseher abzuschalten und zu den Büchern zu greifen. Sie können den Prüfungstermin wenige Wochen im Voraus festlegen. Falls Sie den Termin aber erst einmal gebucht haben und die Vorbereitungen nicht in der geplanten Zeit schaffen, dann müssen Sie den Termin rechtzeitig verlegen, oder Sie verlieren Ihr Geld.

Vorbereitungszeit

Die folgende Tabelle baut auf vielen erfolgreichen CompTIA A+-Examen und den dafür benötigten Vorbereitungszeiten auf. Sie gibt die Menge der Stunden an, die Sie einplanen müssen, um sich auf die CompTIA A+-Examen vorbereiten zu können. Denken Sie daran, dass es sich dabei um durchschnittliche Angaben handelt. Falls Ihnen das Lernen ein wenig schwerfällt oder wenn Sie nervös sind, sollten Sie vielleicht zehn Prozent zu den angegebenen Zeiten hinzuaddieren. Gehören Sie hingegen zu den schnellen Lernern und verfügen über eine Menge Computererfahrung, können Sie von den Zahlen zehn Prozent abziehen!

Kreisen Sie in Tabelle 3 einfach die Zeiten ein, die am besten zu Ihnen passen und addieren Sie sie, sodass Sie schließlich die Anzahl an Vorbereitungsstunden erhalten, die Sie benötigen.

	Erfahrung			
Aufgabenstellung	**Keine**	**Ein- oder zweimal erledigt**	**Ab und zu erledigt**	**Ziemlich oft erledigt**
Adapterkarte installieren	6	4	2	1
Festplatten und SSDs installieren und einrichten	10	8	6	2
Computer mit dem Internet verbinden	8	6	4	2
Drucker und Multifunktionsgeräte installieren	16	8	4	2
RAM installieren	8	6	4	2
CPUs installieren	8	7	5	3
Drucker reparieren	6	5	4	3
Boot-Probleme beheben	8	7	7	5
Tragbare Computer reparieren	8	6	4	2
Mobile Geräte konfigurieren	4	3	2	1
Komplette Systeme aufbauen	12	10	8	6
Mit der Befehlszeile arbeiten	8	8	6	4
Windows installieren/optimieren	10	8	6	4
Mit Windows 7 arbeiten	6	6	4	2
Mit Windows 8/8.1 arbeiten	8	6	4	2
Mit Windows 10 arbeiten	8	6	4	2
Mit Linux arbeiten	8	6	6	3
Mit macOS arbeiten	8	4	4	2
NTFS, Benutzer und Gruppen konfigurieren	6	4	3	2
Drahtloses Netzwerk konfigurieren	6	5	3	2
Software-Firewall konfigurieren	6	4	2	1
Cloud-Dienste nutzen	3	2	2	1
Malware entfernen	4	3	2	0
Diagnosewerkzeuge des Betriebssystems einsetzen	8	8	6	4
Virtuelle Maschinen installieren und konfigurieren	6	4	2	1

Tabelle 3: Analyse der eigenen Fähigkeiten

Addieren Sie zu dem erhaltenen Wert die Stundenanzahl, die Sie anhand der Monate Ihrer unmittelbaren praktischen Erfahrung im PC-Support gemäß Tabelle 4 ermitteln.

Monate direkter praktischer Erfahrung im PC-Support	Ihre Vorbereitungszeit
0	plus 50 Stunden
bis zu 6	plus 30 Stunden
6 bis 12	plus 10 Stunden
mehr als 12	plus 0 Stunden

Tabelle 4: Zeitaufwand für die Prüfungsvorbereitung

Vollkommene Neulinge benötigen meistens ungefähr 240 Stunden Vorbereitungszeit. Ein erfahrener Techniker sollte eigentlich nicht mehr als 60 Stunden benötigen.

Notieren Sie sich hier Ihre errechnete Gesamtvorbereitungszeit: ____________.

Eine Lernstrategie

Nachdem Sie jetzt ein Gefühl dafür bekommen haben, wie lange die Prüfungsvorbereitung etwa dauern wird, wird es Zeit, sich eine Lernstrategie zu überlegen. Ich will Ihnen eine Strategie vorschlagen, die sich, unabhängig davon, ob sie von erfahrenen Technikern oder Neulingen eingesetzt wurde, bei anderen Absolventen der Zertifizierung bereits bewährt hat.

Dieses Buch soll den unterschiedlichen Anforderungen beider Lerngruppen gerecht werden. Bei der ersten Gruppe handelt es sich um erfahrene Techniker, die bereits über umfassende Kenntnisse im PC-Bereich verfügen, sich aber davon überzeugen wollen, dass sie gut auf die spezifischen Themen vorbereitet sind, die in den CompTIA A+-Prüfungen behandelt werden. Bei der zweiten Gruppe handelt es sich um jene Personen, die keine oder nur geringfügige Erfahrungen im Computerbereich haben. Diese können von ausführlichen Erläuterungen der Geschichte und Konzepte der modernen PC-Technologie profitieren und sich so besser an die spezifischen Themen der Prüfungen erinnern. Ich werde kurz von alten und neuen Technikern schreiben, wenn ich diese beiden Gruppen meine. Falls Sie nicht sicher sind, zu welcher Gruppe Sie sich zählen sollen, wählen Sie ein paar Kapitel aus und versuchen Sie, die Fragen am Kapitelende zu beantworten. Wenn Sie weniger als 70 Prozent beantworten können, gehen Sie den Weg für »neue Techniker«.

Die meisten Kapitel habe ich in vier verschiedene Teile unterteilt:

- **Geschichte und Konzepte**: Dieses Wissen gehört nicht zu den CompTIA A+-Prüfungen, hilft Ihnen aber dabei, die Themen der CompTIA A+-Prüfungen besser zu verstehen.
- **1001**: Diese Themen gehören eindeutig zum Wissensgebiet der CompTIA A+-Prüfung 220-1001.
- **1002**: Diese Themen gehören eindeutig zum Wissensgebiet der CompTIA A+-Prüfung 220-1002.
- **Jenseits von A+**: Dies sind eher fortgeschrittene Themen, die wahrscheinlich (noch) nicht in der CompTIA A+-Prüfung vorkommen werden.

Der Anfang der entsprechenden Bereiche wird deutlich mit einer Überschrift wie der folgenden eingeleitet:

Geschichte und Konzepte

Falls Sie zur Gruppe der alten Techniker zählen, können Sie in den jeweiligen Kapiteln alles außer den Teilen zu 1001 und 1002 überspringen. Nach dem Lesen dieser Abschnitte können Sie dann sofort zu den Fragen am Ende des Kapitels übergehen, die sich auf die 1001- und 1002-Abschnitte konzentrie-

ren. Sollten Sie auf Probleme stoßen, arbeiten Sie den Abschnitt *Geschichte und Konzepte* in dem entsprechenden Kapitel durch. Eventuell müssen Sie noch die Abschnitte *Geschichte und Konzepte* früherer Kapitel durcharbeiten, um alle Informationen zu erhalten, die für das aktuelle Thema benötigt werden.

Nachdem Sie alle Kapitel wie beschrieben durchgearbeitet haben, können Sie als alter Techniker direkt dazu übergehen, ihr Wissen anhand kostenloser Übungsprüfungen zu testen. Sobald Sie mehr als 90 Prozent der Fragen beantworten können, sind Sie bereit für die Prüfung. Wenn Sie ein neuer Techniker sind oder als alter Techniker alles lernen wollen, was das Buch zu bieten hat, dann lesen Sie *das ganze Buch* am besten wie einen Roman von der ersten bis zur letzten Seite durch. Springen Sie beim Lesen nicht hin und her. Viele Begriffe und Konzepte bauen aufeinander auf, sodass das Umherspringen leicht zu Frust und Irritationen führen kann, bis Sie dann schließlich das Buch zuklappen und Ihr Lieblingsspiel starten. Nicht, dass ich etwas gegen PC-Spiele hätte, aber diese Fähigkeiten werden für die CompTIA A+-Zertifizierung *nicht* benötigt!

Ihr Ziel beim ersten Durchlesen sollte darin bestehen, die Konzepte und das »Warum« und nicht nur das »Wie« zu verstehen. Beim Lesen ist es sehr hilfreich, wenn Ihnen ein Rechner zur Verfügung steht, sodass Sie zwischendurch einen Blick in den Rechner werfen und eine Hardwarekomponente genauer betrachten oder die praktische Umsetzung eines bestimmten Konzepts prüfen können. Falls Sie beispielsweise gerade etwas über Festplattenlaufwerke lesen, können Sie nämlich gleich einmal die Kabel untersuchen. Sehen sie genauso wie die im Buch beschriebenen aus? Oder gibt es Unterschiede? Und warum? Es ist unverzichtbar, immer genau zu wissen, *warum* Sie jeweils eine bestimmte Aktion durchführen. Beschränken Sie sich nicht einfach nur auf das »Gewusst-wie« einer Aktion! Das dürfte weder in der Prüfung noch bei der praktischen Arbeit als PC-Techniker funktionieren.

Wenn Sie dieses Buch im Rahmen eines Kurses zum Thema »PC-Wartung und Fehlerbehebung« und nicht begleitend zu einem Kurs lesen, der zur Zertifizierungsvorbereitung dient, aber auch dann, wenn Sie bereits über eine gewisse Erfahrung auf diesem Gebiet verfügen, empfehle ich Ihnen dringend, den Weg des neuen Technikers zu wählen. Das Buch enthält eine Menge Details, die zu Stolpersteinen werden könnten, wenn Sie sich nur auf die testspezifischen Abschnitte der Kapitel konzentrieren. Und Sie ergänzen Ihr Lernprogramm neben den praktischen Fähigkeiten um zusätzliches konzeptionelles und geschichtliches Wissen.

In den CompTIA A+-Prüfungen werden grundlegende Anwenderkenntnisse vorausgesetzt. Wenn Sie Pech haben, fallen Sie eventuell mit einer Frage wie der folgenden herein: »Welche Taste müssen Sie beim Verschieben einer Datei aus dem Ordner `C:\DATEN` nach `D:\` mit dem Windows-Explorer gedrückt halten?« Wenn Sie diese Frage beantworten können, ohne zur Tastatur zu greifen und ein paar wahrscheinliche Lösungen auszuprobieren, dann wissen Sie bereits mehr als die meisten Techniker. Bei der praktischen Arbeit können Sie meist durchaus erst ein paar Fehlversuche starten, bevor Sie auf die richtige Lösung zurückgreifen. Für die Prüfungen müssen Sie diese Dinge aber *wissen*! Unabhängig davon, ob Sie zu den alten oder den neuen Technikern zählen, sollten Sie über die für Windows erforderlichen Anwenderkenntnisse verfügen. Dazu gehören die folgenden Themen:

- Der Standarddesktop von Windows und dessen Komponenten (Startmenü, Infobereich usw.)
- Die Manipulation von Fenstern (Größe ändern, verschieben usw.)
- Erstellen, Löschen, Umbenennen und Kopieren von Dateien und Ordnern
- Dateinamenerweiterungen und deren Beziehung zu Programmverknüpfungen
- Gebräuchliche Tastenkombinationen (Hotkeys)
- Windows-Anwendungen installieren, ausführen und beenden

Wenn Sie das Buch erstmals durchlesen, könnten Sie versucht sein, die Abschnitte *Geschichte und Konzepte* zu überspringen. Tun Sie das besser nicht! Wenn Sie die Geschichte und die technologischen Entwicklungen verstehen, die hinter der heutigen PC-Hardware stehen, wird Ihnen auch klar, warum und wie Komponenten funktionieren oder auch nicht. Im Grunde genommen enthalten diese Abschnitte Kenntnisse, die Ihnen ein älterer, erfahrener PC-Techniker vermitteln könnte.

Nachdem Sie das Buch zum ersten Mal gelesen haben, sollten Sie es noch einmal lesen und diesmal kapitelweise von vorne bis hinten durcharbeiten. Wenn Sie ein alter Techniker sind, dann beginnen

Sie an dieser Stelle mit Ihrer Testvorbereitung. Versuchen Sie, in einer Sitzung jeweils ein komplettes Kapitel durchzuarbeiten. Konzentrieren Sie sich dabei auf die 1001- und 1002-Abschnitte. Markieren Sie die Sätze und Stellen, in denen wichtige Dinge behandelt werden. Sehen Sie sich die Abbildungen genau an und achten Sie dabei darauf, wie diese die behandelten Konzepte veranschaulichen.

Lernansätze

Vielleicht ist es bereits einige Zeit her, dass Sie für eine Prüfung lernen mussten. Vielleicht aber auch nicht, und Sie haben nur Ihr Bestes getan, um alle Erinnerungen an diese Erfahrung zu verdrängen! Wie dem auch sei, gewitzte Prüflinge wissen, dass es bestimmte Techniken gibt, durch die das Lernen für Prüfungen effizienter und effektiver wird.

Ein Trick, den Jura- und Medizinstudenten gelernt haben, die sich Unmengen an Daten merken müssen, lautet: Aufschreiben. Wenn man sich etwas aufschreibt (nicht eintippen, sondern *schreiben*), kann man sich besser daran erinnern. Und das gilt selbst dann, wenn man sich das Geschriebene nie wieder ansieht. Machen Sie also möglichst eigene Notizen und zeichnen Sie Abbildungen nach, damit die Informationen sich besser in Ihr Gedächtnis einprägen.

Ein weiterer alter, aber bewährter Trick ist das Erstellen kleiner Karteikärtchen mit Fragen und Antworten zu Themen, die Ihnen schwierig erscheinen. Ein dritter Trick: Nehmen Sie Ihre Aufzeichnungen mit ins Bett und lesen Sie sie kurz vor dem Schlafengehen. Viele Leute stellen fest, dass sie im Schlaf wirklich lernen!

Kontaktadressen

Falls Sie Probleme, Fragen oder einfach nur einen Kommentar loswerden möchten, können Sie auf Englisch eine E-Mail an den Autor (`michaelm@totalsem.com`) oder den Redakteur (`scottj@totalsem.com`) senden.

Alle anderen Informationen erhalten Sie direkt bei der CompTIA über deren Website:
`www.comptia.org`.

Über den Autor

Michael Meyers ist hinsichtlich der CompTIA A+- und der CompTIA Network+-Zertifizierung führender Kopf der Branche. Er ist Vorsitzender und Gründer von Total Seminars, LLC, einem bedeutenden Anbieter von Schulungen zur Wartung von Computern und Netzwerken für Tausende weltweit arbeitender Unternehmen und Mitglied der CompTIA.

Mike Meyers ist Autor einer Vielzahl populärer Bücher (wie denjenigen zum Thema CompTIA A+-Zertifizierung) und Herausgeber verschiedener äußerst erfolgreicher Buchreihen.

Über die weiteren Mitwirkenden

Scott Jernigan hat als Chefredakteur bei Total Seminars auf alles ein wachsames Auge. Scott besitzt den akademischen Grad eines Masters of Arts in der Geschichte des Mittelalters und fühlt sich in den muffigen Archiven Londons ebenso wohl wie im strahlenden Licht des Hauptstandorts von Total Seminars in Houston. Um einem rein akademischen Leben zu entgehen, stürzte er sich Hals über Kopf in Themen der Informationstechnologie und ist als Dozent, Redakteur und Autor tätig.

Scott Jernigan ist selbst Autor vieler Bücher (wie z.B. *Computer Literacy – Your Ticket to IC^3 Certification*) und hat Dutzende weitere redigiert oder Beiträge zu ihnen geleistet. Dabei geht es um Computerthemen wie Hardware, Betriebssysteme, Netzwerke und Zertifizierungen. Zusammen mit Mike Meyers hat er das Buch *Mike Meyers' CompTIA Security+ Certification Guide* geschrieben.

Scott Jernigan hat an allen möglichen Orten in den Vereinigten Staaten Computerkurse geleitet, unter anderem bei den Vereinten Nationen in New York und der FBI-Academy in Quantico. Er lebt, was er lehrt und ist CompTIA A+ und CompTIA Network+ zertifizierter Techniker, Microsoft Certified Professional, Microsoft Office User Specialist und verfügt über Certiport-Internet- sowie Computing-Core-Zertifikate.

Der technische Redakteur **Mark Edward Soper** arbeitet seit mehr als 30 Jahren mit Computern und verwandten Technologien und hat sich durch Schulungen, Schreiben und öffentliche Vorträge auf die technologische Ausbildung spezialisiert. Er ist Autor oder Koautor von mehr als 40 Büchern zu Themen wie CompTIA A+-Zertifizierung, Microsoft Windows, Netzwerke und Fehlerbehebung. Mark Edward Soper hat zudem diese und andere Themen an den verschiedensten Orten in den USA unterrichtet.

Mark Edward Soper verfügt über CompTIA A+- und Microsoft MOS – Microsoft Excel 2013-Zertifizierungen – und gibt derzeit an der University of Southern Indiana und am IvyTech Community College Microsoft-Office-Kurse. Er schreibt auch ein Blog: `http://www.markesoper.com`.

Danksagung

Ich möchte den vielen Leuten danken, die mit ihren Fähigkeiten dazu beigetragen haben, dieses Buch zu ermöglichen:

Scott Jernigan, mein Chefredakteur: Ohne dich hätte ich es nicht geschafft, Amigo. Wahrlich: Gab es jemals eine bessere Partnerschaft als diejenige aus altem Hasen und treuem Gefolgsmann?

Timothy Green, mein Redakteur: Danke für die Zusammenarbeit an einem weiteren großartigen Buch! (Ich bewundere übrigens deine neuen grauen Haare, die vermutlich meiner Unfähigkeit zu verdanken sind, Abgabefristen einzuhalten ...) Aber im Ernst: Mit dir zusammenzuarbeiten war und ist ein wahres Vergnügen.

Laura Stone, Projektleiterin: Danke, Laura, danke, danke, danke, dass du deine Kinder vernachlässigt hast, um mit mir zusammenzuarbeiten. [Hinweis für Leser: Das mit dem Vernachlässigen ist ein Scherz. Laura ist eine hingebungsvolle und ausgezeichnete Mutter.] Ich habe im Laufe der Jahre das Vergnügen der Zusammenarbeit mit vielen Redakteuren gehabt, aber du bist die Crème de la Crème. Santé!

Mark Edward Soper, mein technischer Redakteur: Großartige Arbeit, Mark! Die Zusammenarbeit mit dir war ein Vergnügen. Dank deiner Beiträge und Einsichten ist das Buch viel besser geworden.

Bill McManus, Korrektor: Auch bei dieser Ausgabe wieder eine erstaunliche und exzellente Leistung, Bill. Deine Fähigkeiten erstaunen mich immer wieder. Dankeschön!

Michael Smyer, Technik-Guru und Fotograf: Du hältst mich auf Trab, Michael, mit kleinen und mit großen Dingen. Das Buch ist dadurch viel besser geworden, obwohl ich es noch immer nicht mag, *bei Diskussionen das Nachsehen zu haben.* Die Fotos für dieses Buch sind wieder großartig, dank deines Genies hinter der Kamera. Tolle Leistung!

Dave Rush, Technologe: Ich liebe es, mit dir über Technologie zu diskutieren, Dave. Und deine Forschungskenntnisse verblüffen mich! Danke für all die großartigen Beiträge zu diesem Buch.

Travis Everett, Internet-Guru und Autor: Tolle Beiträge zum Buch, Travis, vom Verfassen der Texte über Nachforschungen bis hin zum Redigieren und der Umbruchkorrektur. Ich freue mich auf viele weitere Projekte.

Dudley Lehmer, mein Partner bei Total Seminars: Wie immer mein Dank dafür, dass du das Schiff auf Kurs gehalten hast, während ich mir die Zeit mit diesem Buch vertrieben habe!

Claire Yee, Akquisekoordinatorin bei McGraw-Hill: Sei immer auf der Hut vor einer leisen Stimme und einem höflichen Lächeln ... Wer hätte gedacht, dass Peitschenhiebe in San Francisco in Houston so schmerzhaft sein können? Danke dafür, dass du uns auf so vielerlei Weise in der Spur gehalten hast.

Janet Walden, redaktionelle Betreuerin bei McGraw-Hill: Es war wieder das reinste Vergnügen, mit dir zusammenzuarbeiten. Ich hätte mir kein besseres Team wünschen können. Tatsächlich habe ich mir das beste Team gewünscht und genau das bekommen!

Richard Camp, Korrekturleser: Fantastische Arbeit!

Sicherheit und Professionalität | 1

Themen in diesem Kapitel:

- Erscheinungsbild und professionelles Auftreten
- Professionelle, produktive Kommunikation mit Kunden
- Sicheres Arbeiten am PC mit den richtigen Werkzeugen

Ich beschreibe mich selbst gern als »Computerfreak« und betrachte es als Kompliment, wenn man mich so nennt. Computerfreaks sind intelligent und nutzen gern neue Technologien. Das sind die guten Aspekte am Wesen der Computerfreaks. Andererseits würden die meisten Leute den Begriff »Freak« als Beleidigung empfinden. Freaks werden in den Medien nur selten positiv dargestellt, und ich glaube zu wissen, warum das so ist. Freaks leiden im Allgemeinen unter ernsten sozialen Schwächen. Diese Schwächen sind klassisch: schlechte Kleidung, Schüchternheit und schlechte Kommunikationsfähigkeiten.

Um Ihnen Ihr Leben und Ihre praktische Tätigkeit zu erleichtern, werden in diesem Kapitel einige der grundlegenden Alltagsfähigkeiten behandelt. Sie werden ein wenig über professionelle Umgangsformen und effektive Kommunikation erfahren. Und wenn Sie die wichtigsten Grundlagen des sozialen Miteinanders kennengelernt haben, werde ich auf einige der Gefahren (z.B. statische Elektrizität) eingehen, denen Sie in Ihrem Beruf begegnen können, und die Hilfsmittel vorstellen, mit denen Sie dieser Herr werden können. Und für die Freaks, die Probleme mit der Ordnung haben oder ständig Geräte beschädigen bzw. sich selbst verletzen, habe ich dann noch einige Tricks, mit denen alles schön ordentlich und sicher bleibt. Das Kapitel endet mit einigen Erläuterungen zur Fehlerbehebung und Sie lernen die CompTIA A+-Strategie zur Fehlersuche kennen – ein ausgezeichnetes Werkzeug, das Ihnen beim Lernen und dem weiteren Werdegang als PC-Techniker gute Dienste leisten wird.

1002

1.1 Der professionelle Techniker

Ein professioneller Techniker zeichnet sich durch Professionalität aus. Das klingt zwar ein wenig abgedroschen, ist aber absolut richtig. Der Techniker glänzt mit professionellem Erscheinungsbild, folgt bestimmten ethischen Grundsätzen und besitzt gewisse Charakterzüge. Sehen wir uns diese Bereiche etwas näher an.

1.1.1 Das äußere Erscheinungsbild

Wir leben in einer zunehmend zwangloseren Gesellschaft. Das Problem daran ist, dass unsere Gesellschaft vielleicht *zu* lässig wird. Viele Kunden bringen lässige Kleidung mit einer allzu lockeren Einstellung in Verbindung. Sie reparieren nicht nur die Computer anderer Leute, sondern machen viel mehr. Sie retten kostbare Familienfotos. Sie halten Kleinunternehmen am Laufen. Das sind bedeutsame Dinge und niemand will, dass eine unsaubere, schludrig gekleidete Person derart wichtige Aufgaben erledigt. Betrachten Sie die Abbildung 1.1. Dabei handelt es sich um unseren hiesigen Zeichner (er hat noch weitere Aufgaben) Ford Pierson, der sich lässig gekleidet hat, um mit seinen Kumpels ein wenig abzuhängen.

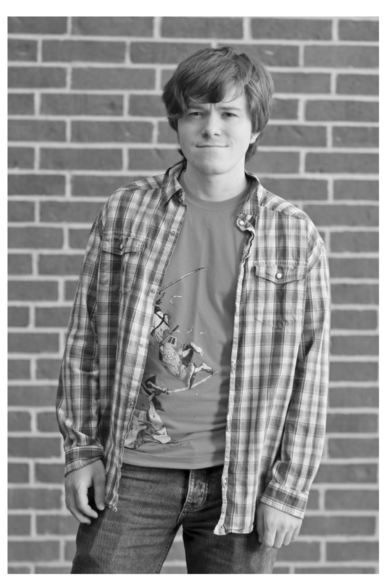


Abb. 1.1: Ford in Freizeitkleidung

Und nun meine Frage: Wenn Sie ein kleines Unternehmen leiten würden und Ihr wichtigster Dateiserver wäre ausgefallen, wodurch 15 Beschäftigte nichts mehr tun können, wie fänden Sie es dann, wenn Ford als Techniker so Ihr Büro betreten würde? Ich hoffe, dass Sie so etwas wie »nicht allzu vertrauenerweckend« antworten werden. In allen Unternehmen gibt es so etwas wie eine *Kleiderordnung* für Techniker. Abbildung 1.2 zeigt Ford in einer recht typischen Bekleidung mit einem Poloshirt des Unternehmens, Khakihose und dunklen Schuhen (das müssen Sie mir schon glauben). Bitte beachten Sie auch, dass Hemd und Hose frei von Knitterfalten sind. Alle Techniker sollten entweder selbst bügeln können oder zumindest wissen, wo sich die nächste Wäscherei befindet.



Abb. 1.2: Ford in Berufskleidung

Haben Sie beim Betrachten dieses männlichen Models bemerkt, dass sein Haar gekämmt und sein Gesicht rasiert ist? Schade, dass ich Ihnen hier keine Gerüche präsentieren kann, aber wenn ich es könnte, dann würden Sie auch bemerken, dass Ford in Berufskleidung auch frisch geduscht ist, ein wenig Deo benutzt hat und dass seine Zähne frisch geputzt sind.

Ich hoffe, dass die meisten Leser jetzt still vor sich hin schmunzeln und das für selbstverständlich halten. Ich habe aber andere Erfahrungen machen müssen. Wenn Sie es das nächste Mal mit einem Techniker zu tun haben, dann fragen Sie sich doch einmal selbst, wie viele dieser einfachen Regeln zum Erscheinungsbild und zur Hygiene er wohl verletzt haben mag. Und machen Sie es sich dann zum Ziel, nicht zu diesen ungepflegten Technikern zu zählen.

1.1.2 Die Charakterzüge eines Technikers

Pfadfinder folgen einem Verhaltenskodex und einem Pflichtenheft. Und selbst wenn Sie selbst nie Pfadfinder gewesen sind, kennen Sie diese Pflichten vielleicht doch: »Ein Pfadfinder ist zuverlässig, treu, hilfsbereit, freundlich, höflich, gütig, gehorsam, fröhlich, sparsam, tapfer, sauber und ehrfürchtig.«

Ich will hier in keiner Weise für die Pfadfinderbewegung werben, mir geht es vielmehr darum, Ihnen zu vermitteln, worum es hier geht, nämlich eine Reihe ethischer Grundsätze, die Ihnen dabei helfen soll, ein besserer Techniker zu werden. Die nachfolgende Liste habe ich zwar selbst zusammengestellt, sie deckt sich aber hervorragend mit den Zielen der CompTIA A+-Zertifizierung. Widmen wir uns also den Pflichten eines Technikers: Ehrlichkeit und Integrität, Zuverlässigkeit und Verantwortungsbewusstsein, Anpassungsfähigkeit und Flexibilität sowie Sensibilität.

Ehrlichkeit und Integrität

Ehrlichkeit und Integrität sind zwar nicht dasselbe, liegen für einen Techniker aber doch derart nahe beieinander, dass man sie unter einem wichtigen ethischen Grundsatz zusammenfassen kann. *Ehrlichkeit* bedeutet letztlich, die Wahrheit zu sagen, während es bei der *Integrität* darum geht, das Richtige zu tun.

Es lässt sich leicht sagen, dass Sie ehrlich sein müssen, aber Sie sollten gewarnt sein, denn das ist in unserer Branche oft gar nicht so leicht. IT-Techniker haben meist mehr Bewegungsfreiheit als andere Berufseinsteiger, was zur Unehrlichkeit verleiten könnte. Zu den größten Versuchungen zählt es, Ihren Chef anzulügen. Ein neuer Techniker, der den ganzen Tag über in einem Kombi herumfährt, könnte sich dazu verleitet fühlen, hinsichtlich der Länge seiner Mittagspause oder der Dauer seiner nächsten Aufgabe die Unwahrheit zu sagen. Dass Sie offen und ehrlich mit Ihrem Chef umgehen sollten, ist aber eigentlich offensichtlich und leicht zu verstehen.

Kunden gegenüber ehrlich zu bleiben, fällt schon viel schwerer. Verkaufen Sie den Leuten keine Waren und Dienstleistungen, die sie nicht brauchen, selbst wenn Sie am Gewinn oder Umsatz beteiligt sind. Belügen Sie Ihre Kunden bei Problemen nicht. Wenn Sie das Problem nicht umgangssprachlich und unmissverständlich erklären können, versuchen Sie nicht, sich in den technischen Jargon (siehe Kasten) zu flüchten. Und wenn Sie etwas einmal nicht wissen, sollten Sie sich auch nicht scheuen, das zuzugeben. Zu viele Techniker denken offenbar, dass es auf einen Mangel an Sachkenntnis hinweisen würde, wenn sie einmal nicht genau wissen, wo das Problem liegen könnte. Ein routinierter Techniker kann auch sagen: »Ich weiß es nicht, aber ich weiß sehr wohl, wie ich es herausfinden und die richtige Antwort geben kann.«

Hinweis

Beim *technischen Jargon* (»Technobabble«) handelt es sich um die (oft sinnlose) Verwendung von Fachausdrücken und Begriffen, mit dem Ziel, sein Gegenüber bei einem technischen Problem einzuschüchtern und zum Schweigen zu bringen.

So wie alle anderen professionellen Dienstleister müssen auch Computertechniker *Integrität* in ihrem Job zeigen. Behandeln Sie alles, was Sie erfahren, als vertraulich und wiederholen Sie es nicht vor anderen Kunden, Kollegen oder Chefs. Beherzigen Sie folgende Regel: »Wenn es sich nicht gerade um ein Schwerverbrechen oder eine direkte physische Gefahr handelt, dann haben Sie auch nichts gesehen«. Mehr zum Umgang mit unerlaubten Inhalten erfahren Sie in Kapitel 27, *Computersicherheit*.

Es gibt eine Ausnahme von dieser Regel. Manchmal müssen Sie zwischen zahlenden Kunden und firmeninternen Benutzern unterscheiden. Ein zahlender Kunde ist jemand, der nicht für Ihr Unternehmen arbeitet und für Ihre Dienstleistungen zahlt. Ein firmeninterner Benutzer ist jemand, der für dasselbe Unternehmen wie Sie tätig ist und Ihre Dienstleistungen nicht direkt bezahlt. Es ist häufig (aber nicht immer) ihre Aufgabe, die Einhaltung firmeninterner IT-Richtlinien zu überwachen. Dazu ein schönes Beispiel. Wenn Sie sich vor Ort bei einem Kunden befinden und bemerken, dass eine Haftnotiz mit dem Kennwort eines Benutzers an dessen Bildschirm klebt, dann sagen Sie nichts. Wenn Sie firmenintern dasselbe beobachten, müssen Sie wahrscheinlich mit dem Benutzer darüber sprechen, dass es gefährlich ist, Kennwörter gut sichtbar preiszugeben.

Sie haben eine Menge Macht, wenn Sie vor dem Computer anderer Menschen sitzen. Sie können leicht private E-Mails lesen, nachsehen, welche Websites sie besucht haben, und vieles andere mehr. Mit einem Klick auf die START-Schaltfläche sehen Sie, welche fünf Programme zuletzt ausgeführt wurden, einschließlich Word und Solitär, und auch, an welchen Dokumenten zuletzt gearbeitet wurde. Lassen Sie das sein. Sie wollen es gar nicht wissen! Und wenn Sie dabei erwischt werden, dass Sie die Privatsphäre eines Kunden verletzen, verlieren Sie womöglich nicht nur Glaubwürdigkeit und Respekt, sondern vielleicht auch Ihren Job. *Respektieren Sie die Privatsphäre und das Eigentum des Benutzers.* Das umfasst auf dem Computer befindliche Dateien, Gegenstände auf dem richtigen Schreibtisch des Benutzers und sogar ausgedruckte Seiten, die im Ausgabefach eines Druckers liegen.

Kennwörter sind ein wichtiges Thema für Techniker. Wir müssen Rechner neu starten, auf Freigaben zugreifen und viele weitere Aufgaben erledigen, für die Kennwörter benötigt werden. Sie sollten es *um jeden Preis vermeiden, die Kennwörter von Benutzern in Erfahrung zu bringen* (siehe Abbildung 1.3). Wenn Sie das für den Zugriff auf einen wichtigen Rechner benötigte Kennwort kennen und dieser kompromittiert wird oder darauf Daten verschwinden, wem wird dann wohl die Schuld gegeben? Bestimmt Ihnen, also wollen Sie die Kennwörter gar nicht wissen! Wenn ein Kennwort nur einmalig erforderlich ist, lassen Sie es vom Benutzer für Sie eingeben. Wenn Sie es mehrfach benötigen (was für gewöhnlich der Fall ist), bitten Sie den Benutzer, es vorübergehend zu ändern.

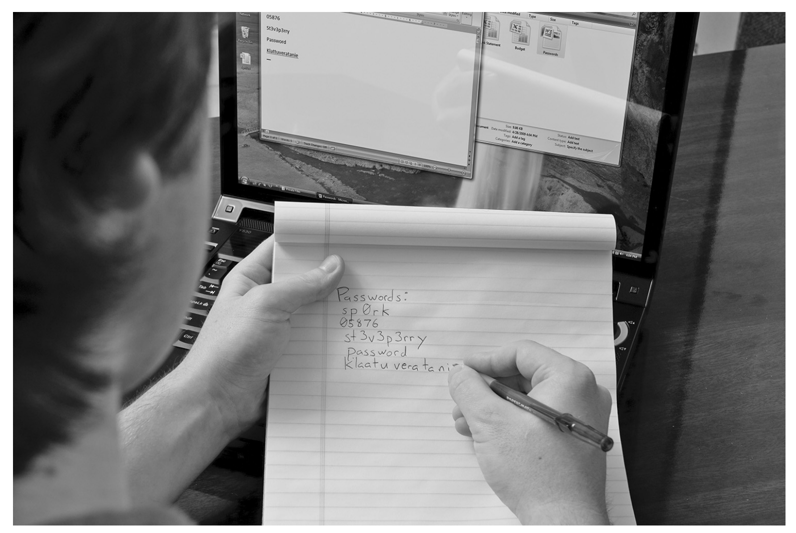


Abb. 1.3: Unterlassen Sie das besser!

Seltsamerweise halten viele Leute die Dinge, die sie bei ihrer Arbeit benutzen, für ihr Eigentum. Georg aus der Buchhaltung spricht bei dem Rechner, den er benutzt, immer von »meinem PC«. Und das Telefon auf dem Schreibtisch von Susi gehört nicht dem Unternehmen, sondern ist »Susis Telefon«. Unabhängig davon, ob dieses Besitzdenken logisch ist oder nicht, müssen Techniker es respektieren. Sie liegen nie falsch, wenn Sie als goldene Regel mit den Dingen anderer Menschen so umgehen, wie Sie sich von anderen Menschen wünschen, dass sie Ihre Dinge behandeln. Verwenden oder berühren Sie nichts – Tastatur, Drucker, Laptop, Bildschirm, Maus, Telefon, Stift, Papier oder Spielzeug –, ohne nicht vorher um Erlaubnis gefragt zu haben. Befolgen Sie diese Regel immer, auch wenn der Kunde gerade nicht zusieht.

Zuverlässigkeit und Verantwortungsbewusstsein

Zuverlässigkeit und *Verantwortungsbewusstsein* sind zwei weitere Charakterzüge, die zwar nicht dasselbe bedeuten, aber oft Hand in Hand gehen. Bei einer zuverlässigen Person kann man sich darauf verlassen, dass sie Handlungen vereinbarungsgemäß ausführt. Verantwortungsbewusste Menschen stehen zu ihren Handlungen. Auch hier sorgt die Bewegungsfreiheit typischer IT-Mitarbeiter wieder dafür, dass Zuverlässigkeit und Verantwortungsbewusstsein äußerst kritische Merkmale sind.

Ein zuverlässiger Techniker erscheint pünktlich zu seinen beruflichen Terminen. Termine platzen zu lassen, ist nicht nur unangenehm, sondern kann für den Kunden auch eine Menge Verlust an Geld, Zeit und Produktivität bedeuten. *Seien Sie also pünktlich.*

Wenn Ihr Arbeitgeber einen Termin für Sie vereinbart, dann erscheinen Sie. Seien Sie dort und lassen Sie nicht zu, dass einfache Probleme (z.B. Verkehrsstaus) Ihr pünktliches Erscheinen verhindern. Nehmen Sie sich ein wenig Zeit für die Vorbereitung. Informieren Sie sich über Hauptverkehrszeiten. Versuchen Sie herauszufinden, ob vorher angesetzte Termine für Probleme sorgen könnten. Es gibt das Sprichwort »Fünf Minuten zu früh ist pünktlich, und pünktlich ist zu spät.« Natürlich kann es manchmal zu Ereignissen kommen, die Ihr pünktliches Erscheinen verhindern. Falls Sie *zu spät kommen sollten, rufen Sie den Kunden unverzüglich an* und teilen Sie ihm möglichst präzise mit, wann Sie schätzungsweise bei ihm sein können. Und eine kleine Entschuldigung kann auch nicht schaden.

Verantwortungsbewusstsein ist ein heikles Thema für IT-Mitarbeiter. Natürlich sollten Sie zu Ihren Taten stehen, aber die Latte liegt spätestens dann ziemlich hoch, wenn es um wichtige Daten und teure Geräte geht. Fragen Sie immer, ob es aktuelle Datensicherungen gibt, bevor Sie an einem Computer arbeiten. Und wenn es keine gibt, dann sollten Sie dem Kunden die Erstellung eines Backups anbieten, auch wenn das für diesen zu höheren Kosten führt. Sollte der Kunde darauf verzichten, dann müssen Sie ihm die Risiken klarmachen, denn dann muss er wissen, dass die Daten auf dem zu reparierenden System gefährdet sein könnten.

Hinweis

Die meisten PC-Reparaturunternehmen verwenden standardisierte Auftragsformulare, die unterschrieben werden müssen und auf denen der Name des Kunden, Rechnungsanschrift und Zahlungsmodalitäten, Datum, Umfang der Arbeiten usw. vermerkt werden müssen. Und selbst wenn Sie auf eigene Rechnung arbeiten, können Ihnen derartige Formulare eine Menge Ärger und Streitigkeiten ersparen. Sie können dazu entweder Ihre eigenen Formulare entwerfen oder im Internet nach Vorlagen suchen.

Sensibilität

Bei der Sensibilität (Einfühlungsvermögen) handelt es sich um die Fähigkeit, sich in die Gefühle und Emotionen anderer Menschen hineinzuversetzen. Sie erfordert eine gute Beobachtungsgabe, ein wenig Zeit und Nachdenken, um menschliche Gefühle einschätzen zu können, und ein Verhalten, das darauf abzielt, dass sich Ihre Klienten wohlfühlen. Ich halte nur wenige der mir bekannten Techniker für besonders sensibel. Die meisten der mir bekannten Nerds (und dabei beziehe ich mich ein) sind eher egozentrisch und merken kaum, was um sie herum vorgeht. Ich will Ihnen aber dennoch ein paar Tipps geben, die ich mit den Jahren gelernt habe.

Machen Sie sich deutlich, dass der Kunde für Ihre Arbeitszeit und Ihre Fähigkeiten zahlt. Sie sollten sich auch darüber im Klaren sein, dass Ihre Anwesenheit unweigerlich bedeutet, dass etwas falsch läuft oder defekt ist, und dass es nur wenige Dinge gibt, über die sich Anwender mehr als über defekte Computer aufregen können. Wenn Sie »dran« sind, müssen Sie wahrscheinlich höchst aufgeregten Kunden zeigen, dass Sie ihren Problemen Ihre volle Aufmerksamkeit widmen. Dazu müssen Sie Ablenkungen vermeiden. Wenn Sie einen persönlichen Anruf erhalten, lassen Sie ihn auf Ihre Voicemail weiterleiten. Wenn Sie berufliche Anrufe erhalten, entschuldigen Sie sich höflich, suchen Sie einen ungestörten Ort auf und halten Sie das Telefonat möglichst kurz. Sprechen Sie nie mit Ihren Kollegen, wenn Ihr Kunde Ihnen dabei zuhören kann. Reden Sie nie schlecht über Kunden. Sie können nie wissen, wann und wo Sie Ihnen das nächste Mal begegnen werden.

Und zu guter Letzt sollten Sie *kulturelles Einfühlungsvermögen* besitzen. Wir leben in einer Welt mit vielfältigen Ethnien, Religionen, Umgangsformen und Traditionen. Wenn ein religiöser Feiertag des Kunden nicht in Ihren Terminplan passt, dann hat der Kunde recht. Wenn der Kunde Sie auffordert, Ihre Schuhe auszuziehen, dann ziehen Sie diese auch aus. Wenn der Kunde von Ihnen verlangt, eine Kopfbedeckung zu tragen, dann tragen Sie eine. *Verwenden Sie gegebenenfalls eine angemessene Berufsbezeichnung.* Wenn Ihr Kunde beispielsweise einen Doktortitel besitzt, verwenden Sie ihn auch, selbst wenn Ihnen das medizinische Fachgebiet unbekannt ist. Bitten Sie im Zweifel Ihren Kunden um Rat bzw. erkundigen Sie sich nach den notwendigen Vorgaben.

1.2 Effektive Kommunikation

Wenn Sie es mit Benutzern, Managern und anderen Eigentümern zu tun haben, die frustriert und aufgeregt sind, weil der Computer oder das Netzwerk nicht funktionieren und sie nicht arbeiten können, müssen Sie in Ihrem Job die Rolle eines Detektivs und Psychologen übernehmen. Man muss wissen, wie man mit aufgeregten Menschen umgeht und wie man Antworten auf Fragen erhält, die sich darum drehen, wie der Rechner in seinen aktuellen Zustand geraten ist. Dabei ist es wichtig, klar und effizient zu kommunizieren.

In diesem Abschnitt betrachten wir effektive Kommunikation. Zunächst geht es um verbindliches Kommunizieren und darum, dem Kunden gegenüber Respekt zu zeigen. Wir untersuchen verschiedene Methoden, dem Benutzer rechtzeitig wertvolle Informationen zu entlocken. Abschließend wird erläutert, wie man die Erwartungen des Kunden zufriedenstellt und wie man professionelle Nachfassaktionen handhabt.

1.2.1 Verbindliche Kommunikation

Häufig werden PC-Probleme durch Fehler oder Nachlässigkeit der Benutzer verursacht. Als Techniker müssen Sie Benutzer auf ihre Fehler aufmerksam machen, ohne sie dabei zu verärgern oder gar mit ihnen zu streiten. Im Rahmen der *verbindlichen Kommunikation* übernehmen Sie weder die Rolle des Lehrmeisters noch des Schwächlings. Bei der verbindlichen Kommunikation zeigen Sie Ihrem Gegenüber zunächst, dass Sie ihn und seine emotionalen Reaktionen verstehen und respektieren. Verwenden Sie Aussagen wie »Ich weiß, wie frustrierend es ist, Daten zu verlieren« oder »Ich weiß, wie ärgerlich es ist, wenn das Netzwerk ausfällt und man seine Arbeit nicht erledigen kann.« Mit Aussagen wie diesen können Sie Kunden beschwichtigen und ihnen vermitteln, dass Sie auf ihrer Seite stehen. Vermeiden Sie es, das Wort »Sie« zu benutzen, denn das kann vorwurfsvoll klingen.

Der zweite Aspekt der verbindlichen Kommunikation besteht darin, dass Sie das Problem korrekt formulieren, ohne den Benutzer dabei direkt zu beschuldigen: »Wie kann sich das Netzwerkkabel während der Mittagspause gelöst haben?« Teilen Sie dem Benutzer schließlich mit, was er tun muss, um Fehler zukünftig zu vermeiden. »Rufen Sie mich an, wenn Sie diesen Summton wieder hören« oder »Sehen Sie vor Neuinstallationen nach, ob sich das Programm auf der Liste des Unternehmens für zulässige Software befindet.« Verwenden Sie immer »Ich« und »mich« und vermeiden Sie Bewertungen. »Ich kann nicht versprechen, dass die Tastatur funktioniert, wenn sie immer so verschmutzt wird.« ist sehr viel besser als »Essen Sie gefälligst keine Kekse mehr am Rechner!«

1.2.2 Respektvolle Kommunikation

IT-Leute sollen generell Menschen bei deren eigentlicher Arbeit im Unternehmen unterstützen. Es ist Ihre Aufgabe, deren Bedürfnisse zu befriedigen, und zwar zur Zufriedenheit Ihrer Klienten und nicht der eigenen.

Sie müssen die Arbeit des Benutzers nicht erledigen, aber Sie sollten sie und die Person als wichtige Teile des Unternehmens respektieren. Sprechen Sie so mit dem Benutzer, wie er bei umgekehrten Rollen mit Ihnen sprechen sollte. Auch dieses Verhalten folgt wieder dem Grundsatz der Gegenseitigkeit.

Sie dürfen nicht erwarten, dass die Welt stehen bleibt, wenn Sie zur Tür hereinkommen, und dass die Arbeit sofort unterbrochen wird, nur damit Sie in Aktion treten können. Obwohl die meisten Kunden ungeduldig sind und Sie bereits erwarten, ist das nicht immer so. Stellen Sie die entscheidende Frage »Kann ich mit meiner Arbeit beginnen?« Geben Sie dem Benutzer Gelegenheit, seine aktuelle Aufgabe zu beenden, sodass Sie ungestört mit Ihrer Arbeit anfangen können.

Gehen Sie auf den Benutzer unter Beachtung der Regeln der höflichen Kommunikation ein. *Nehmen Sie sich die Zeit, ihm zuzuhören. Unterbrechen Sie ihn nicht*, wenn er ein Problem beschreibt. *Hören Sie nur zu und machen Sie sich Notizen.* Möglicherweise hören Sie etwas, was zur Lösung des Problems beiträgt. Formulieren Sie das Problem um und wiederholen Sie es gegenüber dem Kunden, um zu überprüfen, ob Sie die Schwierigkeit verstanden haben (»Der Rechner stürzt also täglich mindestens drei Mal ab?«). Verwenden Sie einen ruhigen und keinesfalls anschuldigenden Tonfall. Natürlich können Sie Fragen des Benutzers beantworten, sollten dabei aber *nicht herablassend oder aggressiv wirken und niemals mit dem Kunden diskutieren.*

Bleiben Sie angesichts des Unheils immer positiv. Gehen Sie nicht in die Defensive, wenn Sie etwas nicht schnell genug herausfinden können und der Benutzer ungeduldig wird. Denken Sie daran, dass der Ärger des Kunden eigentlich nicht Ihnen gilt. Er ist einfach nur frustriert, also nehmen Sie seinen Ärger nicht persönlich. Lassen Sie ihn reden, lächeln Sie, verbreiten Sie Zuversicht und erklären Sie ihm, dass die Fehlersuche bei Computern mitunter einige Zeit dauern kann.

Vermeiden Sie Unterbrechungen von außen, die Sie vom Kunden und der Fehlersuche ablenken könnten. Unterbrechungen können die Fehlersuche enorm verlängern. Außerdem reagieren Kunden leicht beleidigt, wenn Sie Textnachrichten schreiben oder mit Kollegen telefonieren, anstatt den Rechner zu reparieren! Dafür werden Sie nicht bezahlt, deshalb sollten Sie Handys beim Kunden am besten lautlos schalten. Genau für diesen Zweck haben die Technikgötter Voicemail erfunden. Nehmen Sie keine Anrufe entgegen, sofern sie nicht wirklich extrem wichtig sind. Bei möglicherweise wichtigen Anrufen erklären Sie dem Kunden den Notfall, gehen Sie weg und wickeln Sie den Anruf möglichst schnell ab.

Sie sollten während der Arbeit auch keinesfalls soziale Medien nutzen. Facebook aufzurufen oder Tweets abzusetzen, während Ihr Kunde darauf wartet, dass der Computer zum Laufen gebracht wird, ist unhöflich. Und kommen Sie schon gar nicht auf den Gedanken, in sozialen Netzwerken irgendetwas über die Beziehung zu Ihrem Kunden zu schreiben.

Tipp

Wie man in den Wald hereinruft, so schallt es heraus! Mit anderen Menschen so umzugehen, wie Sie von anderen Menschen erwarten, dass sie mit Ihnen umgehen, ist ein weltweit erwünschtes Verhalten. Um dieses Verhalten einzuüben, können Sie es in Situationen ausprobieren, die nichts mit Technik zu tun haben, beispielsweise beim Einkauf im Lebensmittelgeschäft oder dem Laden an der Ecke. Analysieren Sie ganz bewusst, wie die oder der Angestellte hinter dem Tresen von den Kunden behandelt werden möchte. Versetzen Sie sich dann in die Lage des Angestellten. Wie würden Sie sich die Kommunikation der Kunden mit Ihnen wünschen? Handeln Sie dementsprechend!

Wenn Sie erkennen, dass der Benutzer ein Problem unwissentlich oder versehentlich verursacht hat, dann sollten Sie das Problem zwar nicht verniedlichen, aber Sie sollten angesichts des Vorfalls auch

nicht anklagend oder gar beleidigend werden. Wir alle machen Fehler, und diese Fehler sichern Ihnen Ihren Job! *Sie werden bezahlt, weil Menschen Fehler machen und Geräte kaputtgehen.* Es ist nicht unwahrscheinlich, dass Sie in sechs Monaten oder in einem Jahr erneut zu diesem Arbeitsplatz gerufen werden und etwas anderes reparieren müssen. Wenn Sie für den Benutzer zu einem Ansprechpartner werden, dann schaffen Sie dadurch ein besseres Arbeitsumfeld. Wenn ein Benutzerfehler zu dem Problem geführt hat, dann erklären Sie positiv und unterstützend, wie die Aufgabe korrekt erledigt wird. Lassen Sie den Benutzer den Prozess dann nachvollziehen, während Sie ihn dabei unterstützen können.

1.2.3 Antworten erhalten

Ihre Aufgabe als Techniker besteht darin, Computer zu reparieren, und am besten beginnen Sie damit, dass Sie feststellen, was funktioniert und was nicht. Sie müssen erst einmal mit dem Kunden sprechen. Lassen Sie den Kunden das Problem vollständig beschreiben und machen Sie sich dabei Notizen.

Jeder Mensch ist zwar anders, aber die meisten Benutzer mit nicht funktionierenden Computern oder Peripheriegeräten sind ein wenig verzweifelt und gehen möglicherweise defensiv mit dem Problem um. Um diese anfängliche Haltung zu überwinden, müssen Sie die richtigen Fragen stellen *und* sich die Antworten anhören. Anschließend fragen Sie passend nach, mit dem Ziel, *Antworten zu erhalten*, die bei der Lösung des Problems helfen.

Vermeiden Sie in Ihren Fragen Schuldzuweisungen, die Ihnen günstigstenfalls nur nicht weiterhelfen (siehe Abbildung 1.4). Die Frage »Was haben Sie gemacht?« führt meist nur zu der verwirrten oder ängstlichen Antwort »Nichts«, mit der Sie der Problemlösung keinen Schritt näher kommen. Stellen Sie zuerst Fragen zur Klärung der Situation. Sprechen Sie Ihre das Problem betreffenden Vermutungen aus, nachdem Sie die ganze Geschichte des Benutzers angehört haben.



Abb. 1.4: Keine Schuldzuweisungen!

Stellen Sie dann konkretere Fragen, wie z.B. »Wann hat das Gerät zuletzt funktioniert?«, »Hat es je auf diese Weise gearbeitet?«, »Wurde vor Kurzem Software geändert?« oder »Wurde neue Hardware hinzugefügt?« Stellen Sie ergebnisoffene Fragen, um das Problem näher einzukreisen (»Welche Programme liefen gerade, als sich der Rechner aufgehängt hat?«).

Wenn Sie Ihre Fragen freundlich und sachlich halten, erkennt der Benutzer, dass Sie ihm keine Schuld geben und seine Aktionen auch nicht verurteilen (siehe Abbildung 1.5). Sie zeigen ihm, dass Sie dazu

da sind, um ihm zu helfen. Wenn die anfängliche Anspannung erst einmal verflogen ist, bekommen Sie häufig mehr Informationen, wie z.B. darüber, was der Benutzer ausprobiert oder geändert hat. Diese Hinweise können zur schnelleren Lösung des Problems führen.



Abb. 1.5: Bleiben Sie freundlich!

Denken Sie immer daran, dass Sie zwar viel oder vielleicht sogar alles über Computer wissen, der Benutzer aber wahrscheinlich nicht. Das bedeutet, dass er häufig ungenaue und/oder unpassende Begriffe zur Beschreibung von Komponenten oder Funktionen verwendet. Das ist halt so und Sie sollten den Benutzer daher auch nicht unnötig korrigieren. Vermeiden Sie möglichst die Verwendung von Fachjargon, von Akronymen oder Kürzeln aus dem Computerbereich. Dadurch verwirren Sie die bereits aufgeregten Benutzer unnötig und wirken herablassend. Um zu ermitteln, was der Benutzer machen wollte und was passiert ist, als das Problem auftrat, stellen Sie in freundlichem Ton und möglichst in Umgangssprache direkte, sachliche Fragen. Vermeiden Sie Fachausdrücke und bieten Sie visuelle Hilfen. Lassen Sie sich an dem defekten oder einem noch funktionierenden Gerät erklären, was passiert ist.

Sie sollten Benutzer zwar nicht mit Informationen überschwemmen, aber normalerweise wollen sie doch ungefähr und allgemein über Ihre Aktivitäten ins Bild gesetzt werden. Scheuen Sie sich nicht, einfache Analogien oder Konzepte zu verwenden, um ihnen zu vermitteln, was jeweils geschieht. Wenn Sie die Zeit (und das Talent) haben, benutzen Sie Zeichnungen, Komponenten und andere visuelle Hilfen zur Verdeutlichung technischer Konzepte. Wenn ein Kunde technisch interessiert ist und wirklich Antworten bekommen will, vielleicht auch nur, um sich ein Bild von Ihren Kenntnissen zu machen, dann gehen Sie auf ihn ein und weisen Sie ihn auf externe Schulungsangebote hin. Oder empfehlen Sie Ihren Kunden doch ganz einfach dieses Buch!

Natürlich sollten Sie die guten Manieren beherrschen. Ansonsten sollten Sie aber nie davon ausgehen, dass Kunden freundlich oder lässig sind, nur weil Sie das sind. Selbst scheinbar lockere Benutzer erwarten von Ihnen professionelles Verhalten. Im Gegenzug sollten auch Sie es Ihren Kunden nicht erlauben, Sie in unangenehme oder sogar gefährliche oder illegale Situationen zu bringen. Führen Sie während der Arbeit keine Privatgespräche mit Kunden. Führen Sie keine Arbeiten aus, die über den Rahmen Ihres Auftrags hinausgehen, ohne vorher Rücksprache mit Ihrem Vorgesetzten genommen zu haben. (Verweisen Sie die Kunden in diesem Fall möglichst an jemanden, der ihnen helfen *kann*.) Sie sind kein Babysitter und sollten z.B. nicht freiwillig auf Kinder aufpassen, wenn der Kunde sein Büro verlässt. Und wenn der Kunde nicht richtig auf sein Kind aufpasst, sollten Sie auch diese potenziell unsichere Situation nicht tolerieren. Konzentrieren Sie sich darauf, Ihre Arbeit sicher und effizient zu erledigen, und bleiben Sie immer professionell und anständig.

1.2.4 Erwartungen und Nachfassaktionen

Benutzer sind oft sehr besorgt, wenn ihre Rechner und Netzwerke derart zusammenbrechen, dass sie einen Fachmann herbeirufen müssen. Es ist wahrscheinlich, dass sich noch betriebsnotwendige oder zumindest wichtige Daten auf dem Computer befinden. Vielleicht benötigen sie den Rechner auch, um ihre Arbeit erledigen zu können. Wenn sie Geld für professionelle Unterstützung hinblättern, dann gehen sie davon aus, dass Sie ihr System wieder in genau jenen Zustand versetzen, in dem es sich vor dem Auftreten des Fehlers befand. Hoffentlich schaffen Sie genau das. Aber Sie müssen auch auf ihre Erwartungen eingehen und sie wissen lassen, was sie erwarten können.

Sie sollten Ihren Kunden auch nach dem Abschluss Ihrer eigentlichen Aufgabe weiter betreuen. Datensicherungen und die Unterzeichnung von Auftragsformularen (die sehr wichtig sind) haben wir bereits behandelt, aber Sie dürfen auch die Bedürfnisse der Kunden nicht vergessen. Sie wollen doch sicherlich, dass man Sie in guter Erinnerung behält, falls zukünftig erneut Unterstützung gebraucht wird. Dabei sollten Sie an die folgenden Dinge denken.

Zeitrahmen

Wenn Sie dem Kunden eine möglichst genaue Schätzung der Reparaturdauer geben können, dann werden Sie zum Helden. Scheuen Sie sich nicht, mit der Schätzung bis nach der Diagnose des Rechners zu warten. Wenn Sie wirklich nicht wissen, wie lange die Problembehebung dauern wird, dann teilen Sie auch dies dem Kunden mit und sagen Sie ihm auch, was Sie noch wissen müssen, bevor Sie eine Vorhersage treffen können.

Halten Sie sich an den Zeitplan. Wenn Sie schneller fertig werden, toll! Menschen mögen es, wenn etwas schneller als vorhergesagt geht. Wenn Sie den geschätzten Zeitrahmen überschreiten, nehmen Sie Kontakt mit dem Kunden auf und teilen Sie ihm dies möglichst frühzeitig mit. Sagen Sie ihm, was passiert ist, warum der Zeitrahmen überschritten wird, und nennen Sie ihm einen neuen Zieltermin. An dieser Stelle ist es besonders wichtig, dass Sie dem Kunden alle geänderten Umstände mitteilen. Menschen haben Verständnis für Verzögerungen, da sie Teil unseres täglichen Lebens sind. Sie mögen es aber nicht, wenn man sie im Unklaren lässt, insbesondere dann nicht, wenn es dabei um einen wertvollen Rechner geht.

Optionen

Bei vielen Computerproblemen können Sie bei der Behebung auf verschiedene Weise dafür sorgen, dass Schwierigkeiten ähnlicher Art zukünftig nicht wieder auftreten. Letzten Endes geht es dabei um Geld. Bieten Sie Ihrem Kunden, falls möglich, unterschiedliche Lösungen zur Reparatur oder zum Ersetzen eines Geräts an und lassen Sie ihn eine Auswahl treffen.

Bei Lösung A könnte beispielsweise ein defektes Bauteil ersetzt und für den Fall, dass es erneut zu einem Defekt kommt, ein Ersatzbauteil beschafft werden. Bei Lösung B würde das defekte Gerät durch ein besseres Gerät ersetzt, und bei Lösung C käme es zu einem Austausch durch ein identisches Gerät. Bieten Sie mehrere Möglichkeiten an und lassen Sie den Kunden entscheiden.

Dokumentation

Nach Abschluss Ihrer Arbeit dokumentieren Sie das Problem und erfassen dabei den Starttermin, die Lösung (mit Endtermin), die Zahl der benötigten Arbeitsstunden und die ersetzten Teile. Wenn die ersetzten Komponenten dem Kunden gehören, dann händigen Sie ihm diese aus (dies gilt insbesondere für ausgetauschte Speichermedien). Diese Aufzeichnungen können Preise enthalten, müssen es aber nicht.

Nachfassaktionen

Bei Nachfassaktionen handelt es sich üblicherweise einfach nur um einen Telefonanruf, durch den Sie sich davon überzeugen, dass der Kunde mit Ihrer Arbeit zufrieden ist. Damit geben Sie dem Kunden

die Möglichkeit, spezielle Dinge oder Probleme anzusprechen, die möglicherweise vorgefallen sind, und sorgen für den letzten Feinschliff, der bewirkt, dass er sich erneut an Sie wenden wird, sobald er wieder einem technischen Problem begegnet.

1.3 Sicherheit und Werkzeuge

Am *Anfang* der Problemanalyse steht die effektive Kommunikation mit dem Kunden, durch die Sie Einzelheiten zum Problem erfahren und Hinweise darauf erhalten, was gleichzeitig noch geschehen ist. Für die weitere Fehlersuche müssen Sie jedoch den Umgang mit Computern meisterhaft beherrschen. Das beginnt damit, dass Sie sicher mit Computerkomponenten umzugehen wissen und die Werkzeuge des Technikers einsetzen können. Beginnen wir mit einigen der Ihnen möglicherweise begegnenden Probleme und dem Umgang damit.

1.3.1 Elektrostatische Entladung

Alle Computer und Peripheriegeräte verwenden Elektrizität. Solange der Strom wie vorgesehen durch die Leitungen fließt, ist alles in Ordnung. Es kommt jedoch vor, dass elektrische Ladungen von einem Objekt auf ein anderes überspringen und dabei einen Schaden verursachen (ein sogenannter EMP, also ein elektromagnetischer Impuls). Es gibt viele verschiedene Formen von EMPs, wie zum Beispiel Blitze. Wenn ein Blitz in elektronische Geräte einschlägt, ist der ganze Tag im Eimer! Kernwaffenexplosionen erzeugen ebenfalls einen immensen EMP (meine Güte!), aber für Techniker ist vor allem eine Form von Bedeutung, nämlich *elektrostatische Entladungen* (*ESD – ElectroStatic Discharge*). Bei elektrostatischen Entladungen handelt es sich einfach um die Übertragung statischer elektrischer Ladungen von einem Objekt auf ein anderes. Haben Sie schon einmal einen Luftballon an Ihrem Hemd gerieben, damit er an Ihnen kleben bleibt? Das ist ein klassisches Beispiel für statische Elektrizität. Wenn diese statische Ladung überspringt, dann bemerken Sie möglicherweise gar nichts. An kühlen, trockenen Tagen erhalten Sie aber vielleicht beim Berühren eines Türknaufs einen derartigen Schlag, dass Sie einen dicken, blauen Funken überspringen sehen! Ich habe noch nie gehört, dass ein Mensch – abgesehen von dem unangenehmen Schreck – durch elektrostatische Entladungen Schaden genommen hätte. Für Computer gilt das aber nicht. Elektrostatische Entladungen können die empfindlichen PC-Komponenten zerstören, daher ist es unverzichtbar, dass Sie Maßnahmen ergreifen, um sie bei der Arbeit am PC oder anderen computerartigen Geräten zu vermeiden.

Hinweis

Von außen sind alle PCs gut gegen elektrostatische Entladungen geschützt. Solange Sie keinen Schraubendreher in die Hand nehmen und das PC-Gehäuse oder andere computerartige Geräte tatsächlich öffnen, brauchen Sie sich um ESD keine Sorgen zu machen.

1.3.2 Hilfsmittel zur Vermeidung elektrostatischer Entladungen

Elektrostatische Entladungen treten nur dann auf, wenn zwei Objekte miteinander in Kontakt kommen, die unterschiedliche Mengen statischer Elektrizität tragen (man spricht hier von *elektrischen Potenzialen*). Um elektrostatische Entladungen zu vermeiden, müssen Sie »nur« dafür sorgen, dass Sie selbst und die PC-Komponenten, die Sie berühren, dasselbe elektrische Potenzial besitzen, Sie also eine Masseverbindung zum PC herstellen. Das lässt sich z.B. dadurch erreichen, dass Sie sich selbst mit dem PC über ein praktisches, kleines Hilfsmittel verbinden, das *Antistatikarmband* genannt wird. Dieses einfache Hilfsmittel besteht aus einer Leitung, die an der einen Seite mit einer Krokodilklemme und am anderen Ende mit einer kleinen Metallplatte verbunden ist, und wird über ein elastisches Band an Ihrem Handgelenk befestigt. Die Krokodilklemme befestigen Sie an einer blanken Metallstelle des Rechners und das Armband legen Sie sich um eines Ihrer Handgelenke. Abbildung 1.6 zeigt ein typisches Antistatikarmband im praktischen Einsatz.

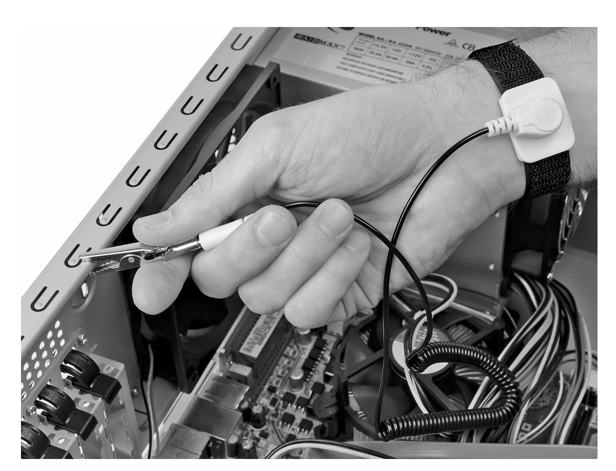


Abb. 1.6: Der richtige Einsatz eines Antistatikarmbands

Wichtig

In trockener, kühler Umgebung ist die statische Elektrizität und damit die Gefahr elektrostatischer Entladungen deutlich erhöht.

Antistatikarmbänder gehören zur Standardausrüstung bei der Arbeit am PC. Aber auch andere Hilfsmittel können nützlich sein. Ein großes Problem bei der Arbeit am Rechner rührt daher, dass oft Komponenten aus dem Rechner entfernt und dann irgendwo abgelegt werden müssen. Wenn Sie eine Komponente aus einem Rechner entfernen, steht sie nicht mehr mit dem System in Verbindung und kann statische Ladungen anderer Quellen übernehmen. Um dieses Risiko zu vermeiden, setzt man *Antistatikmatten* ein. Antistatikmatten sorgen für ein gemeinsames Potenzial. Üblicherweise kauft man eine Kombination aus Antistatikarmband und Antistatikmatte, die miteinander verbunden werden, und die dafür sorgen, dass Sie selbst, der Rechner und alle separaten Komponenten dasselbe elektrische Potenzial aufweisen (Abbildung 1.7).

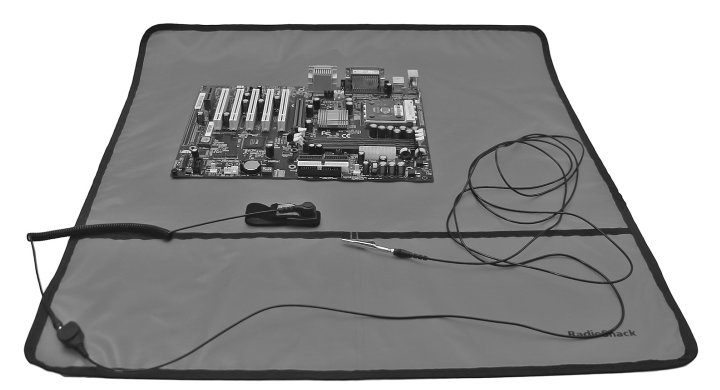


Abb. 1.7: Antistatikarmband und Antistatikmatte

Hinweis

Vergewissern Sie sich, dass die Metallplatte des Antistatikarmbands die Haut Ihres Handgelenks berührt. Befestigen Sie es nicht am Ärmel eines langärmligen Hemds.

Winzige Widerstände – Bauteile, die den Elektrizitätsfluss unterbrechen oder ihm einen *Widerstand* entgegensetzen – in Antistatikarmbändern und Antistatikmatten sorgen dafür, dass keine Ladungen durch die Geräte fließen können. Diese Widerstände können mit der Zeit ausfallen, weshalb es immer ratsam ist, die mit den Antistatik-Hilfsmitteln einhergehende Dokumentation zu lesen und sich darüber zu informieren, wie die winzigen Widerstände zuverlässig geprüft werden können.

Nicht im Rechner befindliche Bauteile müssen in *Antistatikbeuteln* aufbewahrt werden. Dabei handelt es sich um einen speziellen Beutel, der Ihre gesamte statische Elektrizität abschirmt, wenn Sie ihn berühren, damit darin aufbewahrte Komponenten geschützt werden (Abbildung 1.8). Fast alle PC-Komponenten werden beim Kauf in antistatischen Verpackungen geliefert. Erfahrene Techniker werfen diese Verpackungen nicht weg, da man nie wissen kann, wann eine Komponente aus dem Rechner entfernt und für eine Weile im Regal aufbewahrt werden muss.



Abb. 1.8: Antistatikbeutel

Wichtig

Packen Sie Komponenten immer *in* den Antistatikbeutel und legen Sie diese *nicht nur darauf* ab.

Stets ein Antistatikarmband dabei zu haben wäre natürlich ideal, aber die Realität sieht doch ein wenig anders aus. Hin und wieder gerät man in Situationen, in denen die richtigen Antistatik-Hilfsmittel fehlen. Das sollte Sie aber nicht daran hindern, an einem Rechner zu arbeiten. Sie müssen nur besondere Vorsicht walten lassen! Bevor Sie dann mit der eigentlichen Arbeit am Rechner beginnen, sollten Sie zu Beginn und zwischendurch hin und wieder das Netzteil berühren. Wo sich das Netzteil befindet, erfahren Sie in Kapitel 2. Dadurch sorgen Sie dafür, dass das elektrische Potenzial Ihres Körpers und das des Rechners auf dem gleichen Niveau bleiben. Diese Maßnahme zur Selbsterdung ist zwar weniger zuverlässig als das Tragen eines Antistatikarmbands, aber immer noch besser als nichts!

Verwenden Sie also zur richtigen Handhabung von Bauteilen Antistatikarmband, Antistatikmatte, Antistatikbeutel und Selbsterdung.

Tipp: Weitere Geräte zum Schutz vor elektrostatischen Entladungen

Unter bestimmten Umständen ist die Verwendung eines Antistatikarmbands ziemlich unpraktisch. Aus diesem Grund haben die Hersteller verschiedene Alternativen dazu entwickelt. Machen Sie Folgendes:

1. Unternehmen Sie einen Ausflug zu einem örtlichen Computer- oder Elektronikhändler.
2. Sehen Sie sich das Angebot der Antistatik-Hilfsmittel an. Gibt es etwas anderes als Antistatikarmbänder oder Antistatikmatten?
3. Suchen Sie im Internet nach »Antistatik Schutz«. Finden Sie es etwas anderes als Antistatikarmbänder oder Antistatikmatten?
4. Begutachten Sie die Gerätschaften zum Schutz vor elektrostatischen Entladungen. Wiegen Sie die Vor- und Nachteile ab und entscheiden Sie, was Sie in verschiedenen Situationen verwenden würden.

Der letzte Aspekt bei der Vermeidung elektrostatischer Entladungen betrifft die nie enden wollende Frage, ob man den Rechner bei der Arbeit nun vom Stromnetz trennen soll oder nicht. Die Antwort ist eigentlich einfach: Wollen Sie wirklich physisch mit einem Rechner verbunden sein, der an die Wandsteckdose angeschlossen ist? Zugegeben, es ist recht unwahrscheinlich, dass Sie wirklich einen elektrischen Schlag bekommen, aber warum sollte man das Risiko eingehen?

Wichtig

Trennen Sie einen PC immer von der Stromversorgung, wenn Sie Arbeiten im Gehäuseinneren durchführen.

Die Trennung von Spannungsquellen gilt auch für Arbeiten an tragbaren Computern. Trennen Sie das Gerät vom Stromnetz und entfernen Sie den Akku. Bei mobilen Geräten wie Tablets und Smartphones ist das problematisch, weil der Akku oft im Inneren des Geräts fest eingebaut ist. In Kapitel 25 erfahren Sie mehr über die speziellen Anforderungen bei der Arbeit an mobilen Geräten.

1.3.3 EMI (Elektromagnetische Interferenzen)

Wenn ein Magnetfeld elektronische Komponenten stört, dann spricht man von *elektromagnetischen Interferenzen* (*EMI*). Elektromagnetische Interferenzen (Störstrahlungen) sind längst nicht so gefährlich wie elektrostatische Entladungen, können aber einige Komponenten dauerhaft beschädigen und Daten auf bestimmten Speichergeräten löschen. Sie können elektromagnetische Interferenzen verhindern, indem Sie Magnete von Computerausrüstung fernhalten. Bestimmte Komponenten reagieren besonders empfindlich auf elektromagnetische Interferenzen, insbesondere Speichergeräte wie Festplatten.

Das größte Problem im Zusammenhang mit elektromagnetischen Interferenzen besteht darin, dass wir häufig Magnete benutzen, ohne uns dessen bewusst zu sein. Alle Geräte mit einem elektrischen Motor enthalten einen Magneten und auch viele Telefone enthalten Magnete. Lautsprecher und Mikrofone enthalten Magnete. Und auch Netzteile für Laptops und Lautsprecher enthalten Magnete. Sorgen Sie für ausreichende Entfernung zu den elektronischen Komponenten!

1.3.4 RFI (Radio Frequency Interference)

Haben Sie schon einmal seltsame Geräusche gehört, die aus Ihren Lautsprechern kamen, obwohl Sie gar keine Töne wiedergegeben haben? Haben Sie schon einmal seltsame Geräusche in Ihrem Handy gehört? Dann lag dies möglicherweise an *Funkstörungen* (*RFI – Radio Frequency Interference*). Viele Geräte strahlen Funkwellen aus:

- Mobiltelefone (Handys)
- WLAN-Netzwerkadapter
- Schurlostelefone

- Babyfone
- Mikrowellengeräte

Im Allgemeinen sind die von diesen Geräten ausgestrahlten Funkwellen ziemlich schwach und zudem sind die allermeisten elektronischen Geräte hinreichend abgeschirmt, um Funkstörungen zu verhindern. Einige Geräte und insbesondere Lautsprecher reagieren aber empfindlich auf Funkstörungen. RFI führt zwar zu keinen Schäden, kann aber ungemein auf die Nerven gehen. Funkstörungen lassen sich am besten dadurch verhindern, dass man mit Funkwellen arbeitende Geräte möglichst weit entfernt von anderen elektronischen Geräten betreibt.

RFI wird besonders problematisch, wenn zwei Geräte dieselben Frequenzen benutzen. Schnurlostelefone, Babyfone und drahtlose Netzwerke nutzen manchmal dieselben Frequenzbereiche. Und dann stören sie sich zuweilen gegenseitig, was zu schlechter Signalqualität oder sogar völligen Signalausfällen führen kann. Falls möglich, sollten Sie bei einem der Geräte dann eine andere Frequenz einstellen. In Kapitel 20 werden Sie erfahren, wie Sie drahtlose Netzwerke zur Vermeidung von Funkstörungen anders einstellen können.

Hinweis

Die Hersteller von Computerausrüstung verpacken ihre Produkte auf die verschiedenste Weise, um sie vor versehentlicher Beschädigung zu schützen, sei es nun durch physische Beschädigung, ESD, EMI oder RFI. Die typischen, halbdurchsichtigen Beutel sind mit einer Beschichtung versehen, die verhindert, dass sich elektrostatisches Potenzial aufbaut, und schützen den Inhalt auch ein wenig vor Berührungen (und damit auch vor Beschädigung). Zwei Arten metallbeschichteter Beutel bieten Schutz vor EMI, RFI und ESD. Zum einen die silberfarbenen Beutel (wie in Abbildung 1.8), in denen beispielsweise Festplatten verpackt werden, zum anderen die wechselweise schwarz/silbernen Beutel, denen man hin und wieder begegnet.

1.3.5 Werkzeuge

Der grundlegende *Werkzeugsatz* eines Technikers besteht aus einem Kreuzschlitzschraubendreher und vielleicht einem halben Dutzend weiterer Werkzeuge, die Sie gut brauchen können. Die meisten Werkzeugsätze enthalten einen sternförmigen Torx-Schraubendreher, einen Sechskant- und einen Umsteckschraubendreher, eine Pinzette, ein kleines Greifwerkzeug (einen sogenannten *Federarmgreifer*), ein Werkzeug zum Entnehmen von ICs, eine Aderklemme sowie Kreuzschlitz- und Schlitzschraubendreher (Abbildung 1.9).

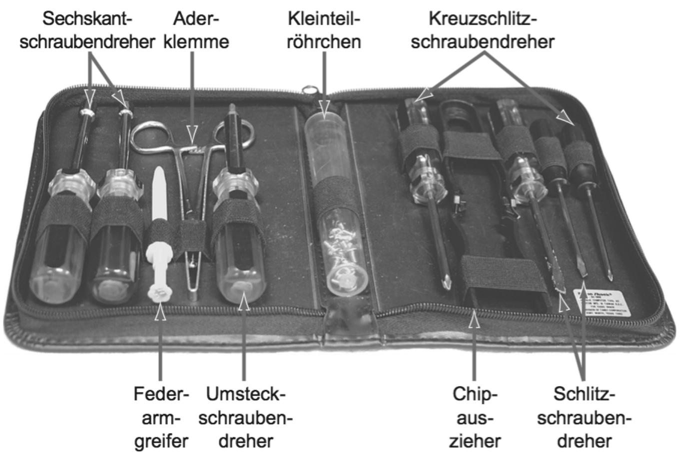


Abb. 1.9: Typische Werkzeugtasche eines PC-Technikers

Viele Techniker fügen noch einen Magnetgreifer hinzu, mit dem sich schwer erreichbare Teile fassen lassen, die ins Gehäuse gefallen sind (eine Ausnahme von der Regel, keine Magnete in die Nähe von Computerausrüstung zu bringen). Viele halten außerdem eine Lupe und eine Taschenlampe für schwer lesbare Ziffern oder Zeichen auf den *Platinen* (*PCB – Printed Circuit Board*) bereit, die einen Großteil der Komponenten innerhalb der Systemeinheit ausmachen. Und ganz anders, als Sie vielleicht denken, brauchen Techniker nur ganz selten einen Hammer.

Für mobile Geräte wie Smartphones oder Tablets sind raffiniertere Werkzeuge erforderlich, wie beispielsweise ein sogenannter Spreizer oder antistatischer Reparaturstift (engl. *spudger*, ist das nicht eine tolle Bezeichnung?). Es sind ganz ausgezeichnete Werkzeugsätze erhältlich. Ich kann die von iFixit (`http://www.ifixit.de`) empfehlen – ich verwende selbst einen (Abbildung 1.10). Diese Werkzeugsätze sind preiswert und zuverlässig. Darüber hinaus bietet iFixit kostenlos Hunderte von Videos an, die zeigen, wie man die Werkzeugsätze verwendet.



Abb. 1.10: Der iFixit-Werkzeugsatz des Autors. Rechts sind einige Spudger erkennbar.

1.3.6 Sicherheit am Arbeitsplatz

IT-Techniker leben in einer gefährlichen Welt. Wir laufen ständig Gefahr zu stolpern, uns Wirbel auszurenken und uns die Finger an heißen Rechnerkomponenten zu verbrennen. Sie müssen auch darauf achten (hinsichtlich der Sicherheit), wie Sie sich kleiden. Nehmen wir uns also ein wenig Zeit, um uns mit diesen Aspekten unserer persönlichen Sicherheit zu befassen und wie wir den daraus resultierenden Gefahren begegnen können.

Vorsicht

Denken Sie daran, dass auch arbeitsrechtliche Schutzbestimmungen zu beachten sind. Möglicherweise gibt es an manchen Arbeitsorten Vorschriften bezüglich bestimmter Schutzkleidung oder weiterer Vorsichtsmaßnahmen. Stellen Sie außerdem sicher, dass bei der Entsorgung alter Komponenten den Umweltschutzbestimmungen Rechnung getragen wird, insbesondere im Fall von Röhrenbildschirmen, Akkus/Batterien und Tonerkartuschen, da diese gefährliche oder giftige Substanzen enthalten können. Fragen Sie im Zweifel bei Ihrem Arbeitgeber oder den örtlichen Entsorgungsbetrieben nach.

Wenn Sie nicht selbst für Ordnung sorgen, dann übernehmen die Hardwarekomponenten mit der Zeit die Herrschaft über Ihr Leben. Abbildung 1.11 zeigt eine Ecke in meinem Büro, in dem das herrscht, was gemeinhin als *Kabelsalat* bezeichnet wird.

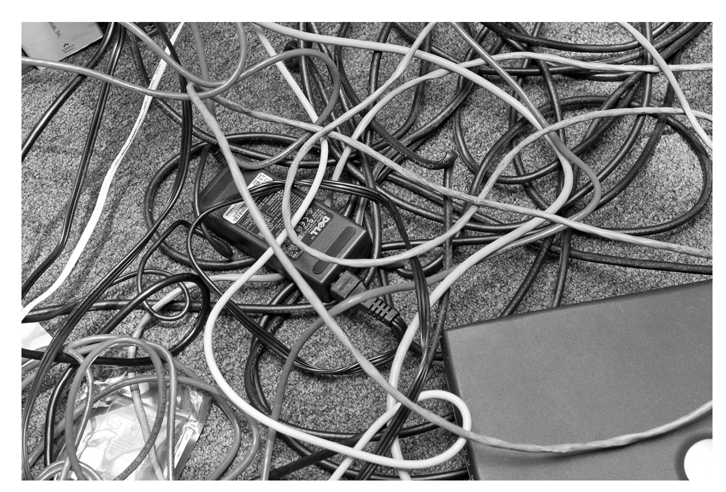


Abb. 1.11: Kabelsalat

Ein solcher Kabelsalat kann zu einer gefährlichen Stolperfalle werden. Während ich das Durcheinander bei mir zu Hause noch tolerieren kann, sind alle Kabel im Unternehmensumfeld sorgfältig hinter den Computergehäusen versteckt oder hinter Wänden bzw. in Kabelkanälen verlegt. Wenn Sie ein Kabel sehen, das eine offensichtliche Stolperfalle darstellt, sollten Sie sich mit der verantwortlichen Person im Hause in Verbindung setzen, damit sie sich sofort darum kümmern kann. Wenn man derartige Gefahren ignoriert, können die Folgen katastrophal sein (Abbildung 1.12). Verlegen Sie die Kabel ordnungsgemäß, um derartige Gefahren zu verhindern.



Abb. 1.12: Dieser Rechner unternimmt eine unfreiwillige Reise.

Bei schweren Kisten handelt es sich um einen weiteren physischen Sicherheitsaspekt. Computer, Drucker, Monitore und damit alles, was wir verwenden, scheint in schweren Kisten angeliefert zu werden. Denken Sie daran, schwere Gegenstände nie aus dem Rücken, sondern immer aus den Beinen heraus zu heben. Und verwenden Sie möglichst immer eine Sackkarre oder andere Transporthilfen. Niemand kann Ihnen so viel bezahlen, dass Sie Ihre eigene Gesundheit riskieren.

Sie müssen sich auch vor heißen Computerkomponenten in Acht nehmen. Es ist schwer, sich zu verbrennen, wenn Sie den Computer, Drucker oder Monitor nicht auch tatsächlich öffnen. Aber dann sollten Sie vor allem auf Komponenten mit Kühlrippen oder anderen Kühlvorrichtungen achten, wie sie in Abbildung 1.13 gezeigt werden. Wenn Sie Kühlrippen sehen, dann ist es wahrscheinlich, dass die Komponenten heiß genug werden, um sich daran verbrennen zu können. Halten Sie auch nach (meist gelben oder roten) Etiketten oder Aufklebern Ausschau, die vor heißen Komponenten warnen. Und zu guter Letzt sollten Sie Ihre Hand im Zweifelsfall den Komponenten so nähern, als ob Sie die Hitze eines Ofens prüfen würden.

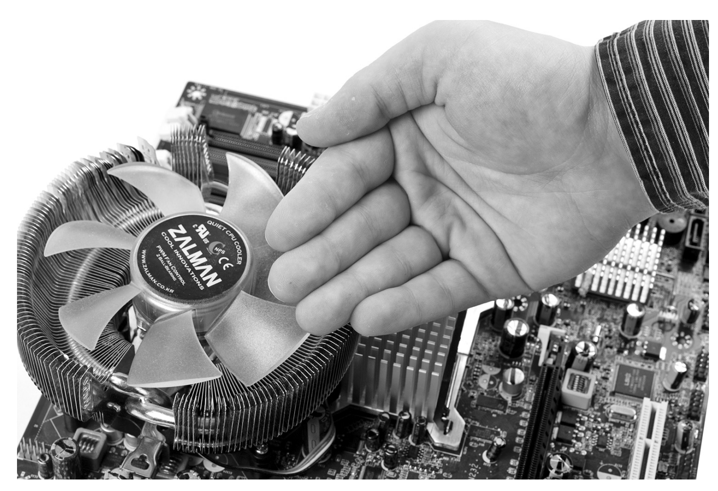


Abb. 1.13: Hier wird vorsichtig geprüft, ob die Kühlrippen heiß sind.

Trennen Sie einen Computer vom Stromnetz, bevor Sie daran arbeiten, sofern möglich. Falls Sie tatsächlich einmal an einem in Betrieb befindlichen Gerät arbeiten müssen, sollten Sie äußerst vorsichtig sein. In Räumen, in denen eine gewisse Feuergefahr besteht, wie etwa in Serverräumen, muss eine geeignete Brandschutzausrüstung vorhanden sein. Die ganze Elektronik und die allgegenwärtige elektrische Spannung stellen eine gefährliche Kombination dar, falls tatsächlich einmal etwas gründlich schiefgeht. Achten Sie auch darauf, dass geeignete Feuerlöscher griffbereit sind.

Wichtig

Wenn Sie Räumlichkeiten für den Betrieb von Computern herrichten, beispielsweise einen Serverschrank oder einen Serverraum (in dem eine Reihe wichtiger Computer betrieben werden), sollten Sie die gebräuchlichen Schutzmaßnahmen ergreifen. Tragen Sie beispielsweise beim Zuschneiden von Trockenbauwänden eine Atemschutzmaske. Setzen Sie eine Schutzbrille auf, wenn Sie Elektrowerkzeug verwenden.

Schließlich sollten Sie, bevor Sie mit der Arbeit an einem Computer beginnen, Schmuckstücke und lose oder weite Kleidung ablegen. Falls Sie lange Haare haben, ziehen Sie es in Erwägung, diese zu einem Pferdeschwanz zu binden. Wenn ein Gegenstand in einen Lüfter gerät oder sich unter einer Komponente festklemmt, ist das sicher nicht in Ihrem Sinn. So ersparen Sie sich – und Ihren Komponenten – jede Menge Ärger.

1.3.7 Strategie zur Fehlersuche

Eine effektive *Strategie zur Fehlersuche* folgt einer Reihe von Schritten, die Sie bei der Diagnose und Reparatur eines Computers in Gedanken durchlaufen. Dazu zählen auch Gespräche mit Anwendern, um herauszufinden, wie und wann das Problem aufgetreten ist, dessen Ursache zu bestimmen, das Testen, Prüfen und Dokumentieren. Techniker verwenden eine Reihe verschiedener Strategien. Wenn Sie die CompTIA A+-Prüfung 220-1001 ablegen wollen, dann haben Sie Glück, denn die CompTIA definiert ihre Ansichten dazu in den Lernzielen klar und deutlich:

5.1 Strategie zur Fehlersuche

1. Identifizieren Sie das Problem.
   - Befragen Sie den Benutzer und stellen Sie fest, ob er Veränderungen am Computer vorgenommen hat. Führen Sie eine Datensicherung durch, bevor weitere Veränderungen stattfinden.
   - Erkundigen Sie sich, ob es Änderungen in der Umgebung oder der Infrastruktur gegeben hat.
   - Überprüfen Sie System- und Anwendungsprotokolle (Logdateien).
2. Stellen Sie eine Theorie der wahrscheinlichsten Ursache auf (und hinterfragen Sie das Offensichtliche).
   - Stellen Sie anhand der Symptome externe oder interne Nachforschungen an, falls erforderlich.
3. Prüfen Sie die Theorie, um die Ursache zu bestimmen.
   - Falls sich die Theorie bestätigt, legen Sie die nächsten Schritte zur Fehlerbehebung fest.
   - Sollte sich die Theorie nicht bestätigen, stellen Sie eine neue Theorie auf oder eskalieren Sie das Problem.
4. Erstellen Sie einen Plan zur Lösung des Problems und setzen Sie ihn um.
5. Überprüfen Sie, ob das System vollständig funktioniert, und treffen Sie bei Bedarf vorbeugende Maßnahmen.
6. Dokumentieren Sie die Befunde, die getroffenen Maßnahmen und die Ergebnisse.

1.3.8 Das Problem identifizieren

Dass Sie vor einem Computer stehen, um ihn zu reparieren, hat einen Grund: Es ist etwas vorgefallen, das dem Computerbenutzer nicht gefällt, und deswegen sind Sie vor Ort. Der erste Schritt beim *Identifizieren eines Problems* besteht im Gespräch mit dem Benutzer. Bitten Sie den Benutzer, Ihnen zu zeigen, was nicht funktioniert. Handelt es sich um einen Fehlercode? Lässt sich auf irgendetwas nicht zugreifen? Reagiert ein Gerät nicht?

Dann stellen Sie dem Benutzer die klassische Technikerfrage (denken Sie an Ihre Kommunikationsfähigkeiten!): »Hat sich irgendetwas am Rechner kürzlich geändert, was dieses Problem hervorgerufen haben könnte?« In Wahrheit meinen Sie: »Haben Sie am Computer herumgespielt? Oder Malware installiert? Haben Sie das USB-Laufwerk mit Gewalt angeschlossen, sodass der Anschluss nun defekt ist?« Natürlich werden Sie solche Dinge niemals laut aussprechen. Fragen Sie einfach nett und freundlich, ohne Benutzer zu beschuldigen, damit sie Ihnen bei der Beseitigung des Problems behilflich sind (Abbildung 1.14).

Erkundigen Sie sich, ob in der Umgebung des Rechners oder an der Infrastruktur irgendwelche Änderungen vorgenommen wurden, die möglicherweise Probleme verursachen.

Bei der Fehlersuche ist es in den meisten Situationen wichtig, dass Sie wichtige Dateien sichern, bevor Sie Änderungen am System vornehmen. In gewissem Maße gehört das zwar zur laufenden Wartung, aber wenn irgendwelche Daten verloren gehen und Sie keine Sicherungskopie erstellt haben, dann können Sie sich ja denken, wem der Anwender die Schuld gibt, oder etwa nicht? Backups kommen in Kapitel 14 ausführlich zur Sprache.

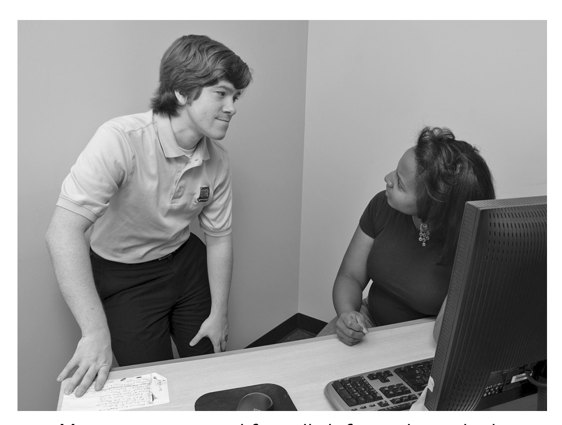


Abb. 1.14: Ein nett und freundlich fragender Techniker

Wichtig

Die CompTIA A+-Prüfungen gehen davon aus, dass Techniker *immer* erst eine Datensicherung durchführen sollten, bevor sie an einem System arbeiten, auch wenn das in der Praxis nicht immer machbar ist.

1.3.9 Theorie der wahrscheinlichsten Ursache

Jetzt ist es an der Zeit, die Probleme zu analysieren und eine dazu passende *Theorie der wahrscheinlichsten Ursache* zu entwickeln. Vielleicht sollte man hier besser von »Vermutungen« sprechen, denn nur die wenigsten Fehler sind derart offensichtlich, dass Sie sofort wissen, was zu tun ist. Greifen Sie auf Ihre Kenntnisse der Verarbeitungsprozesse zurück, um das Problem anhand der auftretenden Symptome zu lokalisieren. Halten Sie Ihre Vermutungen (oder Theorien) einfach. Techniker neigen leider oft dazu, offensichtliche Probleme zu übersehen und sich gleich direkt mit dem System zu befassen (Abbildung 1.15).

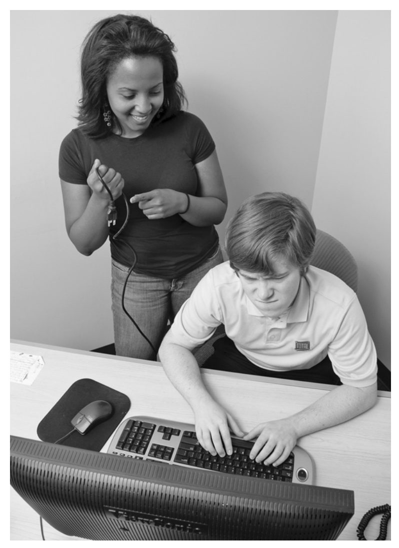


Abb. 1.15: Der Techniker Ford übersieht das Offensichtliche!

Hinweis

In Kapitel 2 wird der Verarbeitungsprozess etwas ausführlicher betrachtet und aufgezeigt, wie alles ineinandergreift, damit es funktioniert. Eine gründliche Fehlersuche und elementare Kenntnisse des Verarbeitungsprozesses sind bei der Fehlerbehebung von entscheidender Bedeutung.

1.3.10 Nachforschungen

In vielen Situationen ist es erforderlich, auf zusätzliche Ressourcen zurückzugreifen, um die wahrscheinlichste Ursache des Problems aufzuspüren. Sie sollten daher, sofern das nötig ist, anhand der auftretenden Symptome externe oder interne Nachforschungen anstellen.

Das Internet ist buchstäblich jederzeit zur Hand, wenn man mittels Smartphone oder Tablet darauf zugreifen kann, um eine kurze Internetrecherche durchzuführen, die womöglich unverzüglich zur Lösung technischer Probleme führt. Wenn beispielsweise auf dem Bildschirm des Benutzers eine Fehlermeldung angezeigt wird, sollten Sie mit einer Suchmaschine nach dem vollständigen Text suchen.

Mit einer internen Nachforschung ist gemeint, andere Techniker vor Ort um Hilfe zu bitten. Prüfen Sie, ob es firmeninterne Aufzeichnungen zu den einzelnen Computern gibt (beispielsweise in einer Fehlerdatenbank, in der früher aufgetretene Problemfälle eingetragen worden sind). Auf diese Weise können Sie herausfinden, ob es beim betroffenen Computer oder einem bestimmten Benutzerverhalten bekannte Probleme gibt.

1.3.11 Außerhalb des Gehäuses

Nehmen Sie sich vor dem Öffnen des Gehäuses einen Augenblick Zeit für die Suche nach Hinweisen. Und – noch wichtiger – nutzen Sie dabei all Ihre fünf Sinne.

Was sehen Sie? Ist ein Stecker oder ein Plastikbauteil offensichtlich defekt? Selbst wenn Stecker oder Bauteil noch funktionieren, könnte die physische Beschädigung zusätzliche Hinweise liefern. Wenn sich der Benutzer nicht mit dem Netzwerk verbinden kann, überprüfen Sie das Kabel. Wurde es möglicherweise von einem Gegenstand überrollt, wodurch die feinen Drähte im Kabel Schaden genommen haben? Sind da etwa Reste von Marmelade an der verklemmten Schublade des optischen Laufwerks zu sehen? Eine äußerliche Sichtprüfung des Computers ist wichtig.

Fühlt sich die Systemeinheit heiß an, wenn Sie diese mit der Hand berühren? Sind die Lüfter hörbar oder deren Vibrationen spürbar? Falls nicht, würde dies auf einen überhitzten (oder kurz davor stehenden) Computer hinweisen. Moderne Computer laufen zwar oft auch noch, wenn sie sehr heiß geworden sind, werden dann aber normalerweise sehr lahm.

Wenn Sie einen Augenblick auf die Geräusche des PCs achten, könnte Ihnen das ebenfalls Hinweise auf die Ursache des Problems geben. Ein korrekt funktionierender Computer gibt nur wenige Geräusche von sich, lediglich ein gleichmäßiges Surren der sich drehenden Lüfter. Sollten Sie klickende oder schleifende Geräusche hören, sind das keine gute Zeichen und ein äußerst wichtiger Hinweis! In den Kapiteln 8 und 9 befassen wir uns eingehender mit Festplatten – sie sind für gewöhnlich die Verursacher klickender oder schleifender Geräusche.

Und schließlich sollten Sie auch Ihre Nase nicht vergessen. Wenn Sie den unverkennbaren Geruch von Ozon wahrnehmen, dann wissen Sie, dass dies ein untrüglicher Hinweis auf durchgebrannte oder schlicht zu heiße elektronische Komponenten ist.

1.3.12 Die Theorie prüfen, um die Ursache zu bestimmen

Gut, nun haben Sie sich also für eine einleuchtende Theorie entschieden. Jetzt müssen Sie sich davon überzeugen, dass Ihre Theorie tatsächlich zum aktuellen Problem passt, und überprüfen, ob sich das Problem damit beheben lässt. Die größte Herausforderung bei der Reparatur von Computern besteht

darin, dass die Theorie quasi erst durch die geglückte Reparatur bestätigt wird. In vielen Fällen führt eine Überprüfung der Theorie lediglich zur Bestätigung, dass tatsächlich irgendetwas defekt ist. In diesem Fall ersetzen Sie das defekte Bauteil einfach.

Sollten Sie mit Ihrer Theorie nicht weiterkommen, müssen Sie eine neue entwickeln und sie überprüfen. Wenn sich die Theorie bestätigt und Sie den Fehler beheben können: Großartig!

An dieser Stelle müssen Sie sich allerdings bei Ihrem Vorgesetzten vergewissern, dass es Ihnen auch gestattet ist, die erforderlichen Maßnahmen durchzuführen. Schenken Sie immer den Richtlinien und Vorschriften Ihrer Firma Beachtung und ziehen Sie die Folgen in Betracht, bevor Sie Änderungen vornehmen. Wenn Sie gerade mit beiden Armen im Inneren eines Rechners zugange sind und Ihr Chef kommt zufällig vorbei und fragt »Wer hat Ihnen das erlaubt?«, könnte das ein unerfreulicher Tag werden!

Wenn Sie nicht in der Lage sind oder es Ihnen nicht erlaubt ist, das Problem zu beheben, müssen Sie das Problem *eskalieren*.

Bei der *Eskalation* handelt es sich um einen Vorgang in Ihrem Unternehmen (oder manchmal auch nur um Ihre Entscheidung), der dann durchlaufen wird, wenn eine mit einer Reparatur beauftragte Person den Auftrag selbst nicht erledigen kann. An der Eskalation gibt es nichts auszusetzen, denn niemand kann alle Probleme beheben. In allen Unternehmen sollte es bestimmte Vorgehensweisen bei der Eskalation geben. Das könnte ein einfacher Anruf bei Ihrem Chef sein. Dabei müssen Sie möglicherweise ein internes Formular ausfüllen und an eine andere Abteilung weiterleiten. Manchmal wird aber auch eher formlos eskaliert. Vielleicht wollen Sie erst einmal online Nachforschungen zum Problem anstellen oder zunächst in der internen Dokumentation nachsehen, ob das Problem in der Vergangenheit schon einmal aufgetreten ist. (Lesen Sie dazu auch den Abschnitt 1.3.15, *Dokumentation der Befunde, Maßnahmen und Ergebnisse*, weiter hinten in diesem Kapitel.) Vielleicht wollen Sie auch nur einen Mitarbeiter hinzuziehen, der sich mit dem aufgetretenen Problem besser auskennt (Abbildung 1.16).



Abb. 1.16: Der Techniker Ford bittet Scott um Hilfe.

1.3.13 Vorgehen planen

Inzwischen haben Sie eine ziemlich genaue Vorstellung von dem Problem und auch, welche Befugnisse zur Behebung erforderlich sind. Sie müssen Ihr *Vorgehen planen*, um das Problem zu beheben und die Lösung umzusetzen. Manchmal sind dazu mehrere Schritte notwendig. Vielleicht benötigen Sie zusätzliche Ressourcen, wie etwa zuverlässig funktionierende Ersatzteile. Ein Backup der Benutzerdaten sollte ebenfalls Bestandteil des Plans sein.

1.3.14 Überprüfung und vorbeugende Maßnahmen

Fantastisch! Durch Ihre eigene sorgfältige Arbeit oder Eskalation haben Sie das Problem gelöst oder glauben es zumindest. Beachten Sie hier zwei Punkte. Erstens könnte es sein, dass *Sie* das Problem zwar für gelöst halten, der Benutzer oder der Kunde in dieser Hinsicht aber vielleicht ganz anderer Ansicht ist. Und zweitens sollten Sie möglichst vorbeugende Maßnahmen ergreifen, die dafür sorgen, dass das Problem zukünftig nicht erneut auftritt.

Überprüfung, ob das System vollständig funktioniert

Durch die Überprüfung, ob das System wieder vollständig funktioniert, können Sie gewährleisten, dass Ihre Anwender glücklich und zufrieden sind. Angenommen, ein Anwender kann nicht drucken. Sie stellen fest, dass die Druckerwarteschlange wegen eines hängenden Laserdruckers angehalten wurde. Sie starten den Drucker neu und die Druckaufträge werden ausgegeben. Auftrag erledigt, nicht wahr?

Am besten lässt sich die volle Systemfunktionalität dadurch überprüfen, dass man den Benutzer ein paar Minuten lang seine üblichen Aufgaben ausführen lässt und dabei zusieht. Kleinere Fehler werden dabei schnell erkannt und Sie erhalten zudem einen interessanten Einblick in die Arbeitsweise des Benutzers. Für gute Techniker ist es entscheidend, dass sie wissen, was ihre Benutzer tun, denn nur dann können sie ihnen dabei helfen, ihre Arbeit besser zu erledigen (Abbildung 1.17).

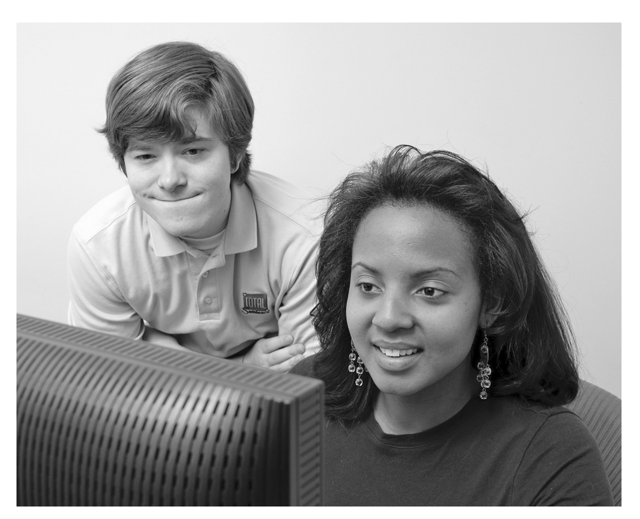


Abb. 1.17: Der Techniker wartet ab und beobachtet.

Bei Bedarf vorbeugende Maßnahmen treffen

Ein sehr erfahrener Techniker sagte mir einmal, dass das Ziel des wirklich guten Support-Technikers darin bestünde, seinen Stuhl nicht mehr verlassen zu müssen. Das ist zwar ein ziemlich hochgestecktes Ziel, ergibt aber durchaus einen Sinn. Unternehmen Sie alles, damit sich ein Problem nicht wiederholt. In einigen Fällen liegt es auf der Hand, was zu unternehmen ist, beispielsweise dass Sie dafür sorgen, dass Anti-Malware-Software auf einem Rechner installiert ist, damit er sich nicht erneut infiziert. Manchmal gibt es aber auch gar keine Maßnahmen, die man ergreifen könnte, denn schließlich lässt sich nicht verhindern, dass Festplatten manchmal ihren Geist aufgeben. Eine vorbeugende Maßnahme lässt sich jedoch in fast allen Fällen treffen: die Schulung der Anwender. Nutzen Sie die Zeit, die Sie bei Anwendern verbringen, um sie formlos über Probleme zu unterrichten. Zeigen Sie die Gefahren schädlicher Software auf oder erklären Sie, dass Festplatten letzten Endes Verschleißteile sind und manchmal eben ausfallen. Je mehr Ihre Benutzer wissen, desto seltener müssen Sie Ihren Stuhl verlassen.

1.3.15 Dokumentation der Befunde, Maßnahmen und Ergebnisse

Angesichts seines berühmten Ausspruchs »Wer sich nicht seiner Vergangenheit erinnert, ist dazu verurteilt, sie zu wiederholen«, glaube ich, dass der Philosoph und Schriftsteller George Santayana ein hervorragender Techniker gewesen wäre. Für Techniker sollte die Dokumentation der letzte Schritt jeder Fehlerbehebung sein. Diese Dokumentation muss in einigen Unternehmen strengen formalen Anforderungen genügen, es kann sich aber auch einfach nur um ein paar Notizen handeln, die Sie für sich selbst machen. Sie müssen Ihre Tätigkeit aber dokumentieren! Was war das Problem? Durch welche Maßnahmen konnten Sie es beheben? Was hat funktioniert? Was nicht? Den besten Leitfaden für die Dokumentation liefert die folgende Frage: »Was hätte ich über das Problem gern gewusst, bevor ich mich mit ihm befasst habe?« Eine gute Dokumentation ist der beste Hinweis auf einen guten Techniker (Abbildung 1.18).

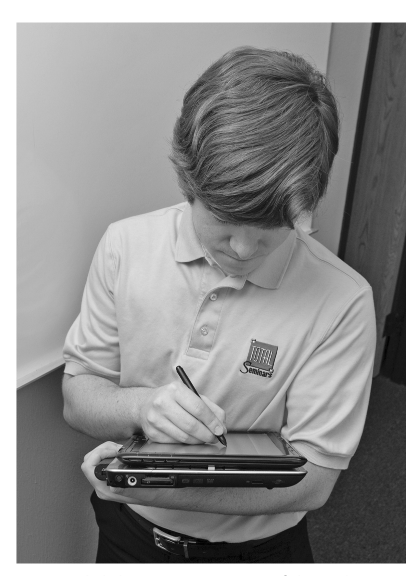


Abb. 1.18: Ford dokumentiert eine erfolgreiche Reparatur.

Die Dokumentation von Problemen hilft Ihnen, den Fehlerverlauf eines Rechners zu beobachten, sodass Sie langfristig Entscheidungen treffen können, wie beispielsweise die Ausmusterung eines Rechners oder weiterreichende Reparaturen. Wenn Sie und Ihre Kollegen mehrere Male eine bestimmte Reparatur an Susis Computer ausgeführt haben, würden Sie sich vielleicht dazu entschließen, das System komplett auszutauschen, statt die Reparatur noch ein viertes Mal durchzuführen.

Die Dokumentation hilft Ihren Kollegen, wenn sie eine Aufgabe fertigstellen müssen, die Sie nicht abgeschlossen haben, oder wenn sie auf einem Rechner, den Sie schon einmal repariert haben, nach einem Fehler suchen. Und auch die umgekehrte Richtung trifft zu. Wenn Sie einen Anruf bekommen, dass Franks Computer kaputt ist, und die Aufzeichnungen prüfen, um festzustellen, ob es bereits Serviceanfragen für diesen Computer gab, stellen Sie möglicherweise fest, dass die Reparatur für ein bestimmtes Problem bereits dokumentiert ist. Das gilt vor allem bei vom Benutzer verursachten Problemen. Wenn Sie dokumentieren, was Sie repariert haben, müssen Sie sich auch nicht auf Ihr Gedächtnis verlassen, wenn Ihr Kollege Sie fragt, was Sie gegen das merkwürdige Problem unternommen haben, das letztes Jahr auf Sabines Computer auftrat.

Die Dokumentation ist auch von großer Bedeutung, wenn Ihnen oder einem Benutzer vor Ort ein Unfall zustößt. Wenn Ihr Kollege Ralph beispielsweise einen Bildschirm auf seinen Fuß hat fallen lassen und der Bildschirm kaputt und der Fuß gebrochen ist, müssen Sie einen *Unfallbericht* ausfüllen, wie bei jedem anderen Unfall auch, sei es nun ein Stromschlag, ein Chemieunfall oder ein sonstiger Perso-

nenschaden. Der Unfallbericht sollte genau beschreiben, was geschehen ist und an welchem Ort. Auf diese Weise können Ihre Vorgesetzten schnelle und wirksame Maßnahmen ergreifen.

1.4 Wiederholung

1.4.1 Fragen

1. Welche der folgenden Kleidungsstücke eignen sich am besten für den Arbeitsplatz? (Wählen Sie zwei Antworten aus.)
   A. Saubere, gebügelte Khakihose
   B. Sauberes, faltenfreies T-Shirt
   C. Sauberes, faltenfreies Polohemd
   D. Saubere, gebügelte Jeans
2. Sie erhalten einen Anruf von einem verzweifelten Anwender, der sagt, dass sein Bildschirm leer bleibt. Welche Fragen könnten Sie ihm daraufhin stellen? (Wählen Sie zwei Antworten aus.)
   A. Ist der Computer eingeschaltet?
   B. Ist der Monitor eingeschaltet?
   C. Haben Sie den Rechner neu gestartet?
   D. Was haben Sie gemacht?
3. Welches Werkzeug gehört in die Werkzeugtasche eines jeden Technikers?
   A. Zange
   B. Hammer
   C. Schlitzschraubendreher
   D. Kreuzschlitzschraubendreher
4. Wann ist es angemessen, einen Benutzer anzuschreien?
   A. Wenn er denselben Bock zum zweiten Mal baut.
   B. Wenn er Sie bei der Suche nach der Problemursache unterbricht.
   C. Wenn er denselben Bock zum fünften Mal baut.
   D. Nie.
5. Bei der Suche nach einem Softwareproblem an Paulas Computer hören Sie sich ihre Problembeschreibung an. Währenddessen erhalten Sie eine Textnachricht von Ihrem Chef. Was wäre jetzt die geeignetste Maßnahme?
   A. Entschuldigen Sie sich, verlassen Sie das Büro und antworten Sie Ihrem Chef.
   B. Schnappen Sie sich Paulas Telefonhörer und wählen Sie die Nummer Ihres Chefs.
   C. Warten Sie, bis Paula ihre Beschreibung beendet hat, und fragen Sie sie dann, ob Sie ihr Telefon benutzen dürfen, um bei Ihrem Chef anzurufen.
   D. Warten Sie, bis Paula ihre Beschreibung beendet hat, führen Sie alle einfachen Reparaturversuche aus, und erklären Sie ihr dann, dass Sie Ihren Chef über Ihr Handy anrufen müssen.
6. Sie befinden sich am Arbeitsrechner eines Kunden, um einige Software- und Hardwareupdates zu installieren. Das dauert eine Weile und erfordert einige Rechnerneustarts. Was sollten Sie hinsichtlich des Kennworts für das Benutzerkonto machen?
   A. Bringen Sie den Kunden dazu, sich während der benötigten Zeit neben Sie zu setzen, damit er das Kennwort jeweils eingeben kann.
   B. Bitten Sie den Benutzer dazu, sein Kennwort aufzuschreiben, damit Sie es benutzen dürfen.
   C. Bitten Sie den Benutzer, sein Kennwort vorübergehend zu ändern, damit Sie es benutzen können.
   D. Rufen Sie Ihren Vorgesetzten an.

7. Welche der folgenden Nachfassaktionen empfiehlt sich nach der Problembehebung nach einem telefonischen Außenauftrag?
   A. Sie telefonieren nach ein paar Tagen mit dem Kunden und überzeugen sich davon, dass der reparierte Computer tadellos funktioniert.
   B. Sie notieren sich alle verwendeten Kennwörter, um sie für spätere Einsätze gleich griffbereit zu haben.
   C. Sie notieren sich die Namen und Daten aller besonders wichtigen Personen, denen Sie begegnet sind, um sie für spätere Einsätze parat zu haben.
   D. Sie machen nichts. Sie haben Ihre Arbeit schließlich erledigt.
8. Durch welches Hilfsmittel können Sie versehentliche statische Entladungen vermeiden und dafür sorgen, dass Sie dasselbe elektrische Potenzial wie der Computer besitzen, an dem Sie gerade arbeiten?
   A. Antistatikspray
   B. Antistatikbeutel
   C. Antistatikarmband
   D. Kreuzschlitzschraubendreher
9. Was sollten Sie machen, nachdem Sie das beim Rechner vorliegende Problem ermittelt und die wichtigen Daten gesichert haben?
   A. Eine Theorie der wahrscheinlichsten Ursache entwickeln.
   B. Mit der Reparatur des Rechners beginnen.
   C. Dem Benutzer weitere Fragen stellen, um festzustellen, wie er das Problem verursacht hat.
   D. Das Problem dokumentieren.
10. Was müssen Sie nach erfolgreicher Reparatur eines Rechners unbedingt machen?
   A. Gar nichts, der Auftrag ist erledigt.
   B. Den Benutzer ermahnen, weil er der IT-Abteilung so viel Arbeit beschert hat.
   C. Die eigenen Befunde dokumentieren.
   D. Den Rechner so verriegeln, dass der Benutzer dieselben Probleme nicht erneut verursachen kann.

1.4.2 Antworten

1. **A, C.** Khakihose und Poloshirt sind immer besser als Jeans und T-Shirt.
2. **A, B.** Klären Sie erst die einfachsten Möglichkeiten. Bei einem leeren Bildschirm prüfen Sie erst einmal, ob Rechner und Bildschirm eingeschaltet sind.
3. **D.** Ein Techniker sollte wenigstens einen Kreuzschlitzschraubendreher dabei haben.
4. **D.** Sie sollten auf Kunden nie wütend werden und sie niemals anschreien.
5. **D.** Konzentrieren Sie sich auf die Kundin und benutzen Sie nicht ihre Geräte.
6. **C.** In dieser Situation bitten Sie am besten um ein temporäres Kennwort. Sorgen Sie vor dem Weggehen dafür, dass der Anwender sein Kennwort wieder ändert.
7. **A.** Eine einfache Nachfassaktion sorgt für Wohlwollen und Vertrauen. Dabei handelt es sich um eine sehr wichtige Aktion nach dem Abschluss eines Auftrags.
8. **C.** Ein Antistatikarmband sorgt dafür, dass Sie selbst dasselbe elektrische Potenzial wie der Computer besitzen.
9. **A.** Wenn Sie das Problem festgestellt und wichtige Daten gesichert haben, sollten Sie eine Theorie der wahrscheinlichsten Ursache entwickeln.
10. **C.** Nach Abschluss einer Reparatur sollten Sie immer Ihre Befunde dokumentieren.

Der gläserne PC | 2

Themen in diesem Kapitel:

- Funktionsweise eines PCs
- Steckverbinder, Anschlüsse und Geräte eines typischen Computersystems
- Gemeinsamkeiten verschiedener Betriebssysteme

Charles Babbage (Abbildung 2.1) hatte eigentlich gar nicht vor, die Welt zu verändern. Er wollte lediglich einige Berechnungen anstellen, ohne sich dabei Sorgen um menschliche Fehler machen zu müssen – seinerzeit kam das nur allzu häufig vor. Babbage war ein Mathematiker des 19. Jahrhunderts. Damals konnte sich noch niemand vorstellen, elektronische Taschenrechner zu bauen. Wenn er sich mit komplizierter Mathematik befasste, waren die besten verfügbaren »Computer« Menschen, die handschriftlich rechneten und Gleichungen mit Papier und Bleistift lösten.

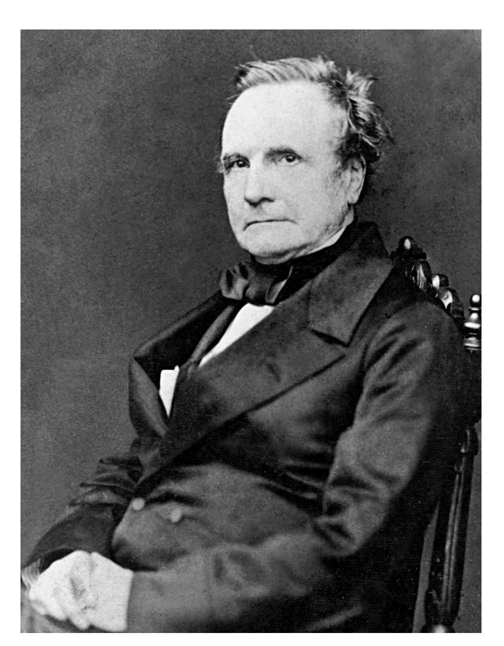


Abb. 2.1: Charles Babbage, der Vater des Computers

Babbage wollte Maschinen konstruieren, die Berechnungen mechanisch ausführen können, damit es nicht zu Rechenfehlern kommen kann. Er war seiner Zeit mit diesen Gedanken weit voraus, denn Mitte des 20. Jahrhunderts wurden seine Ideen von Erfindern wieder aufgegriffen, die riesige rechnende Maschinen bauten, die sie *Computer* nannten.

Dieses Kapitel stellt Ihnen vor, wie Computer und computerähnliche Geräte funktionieren. Zunächst betrachten wir, wie Berechnungen eigentlich ausgeführt werden. Dann wenden wir uns den Hardwarekomponenten zu, die in allen Geräten vorkommen. Das Kapitel schließt mit Erläuterungen zu der Software, die in allen Betriebssystemen Verwendung findet und bestimmten Funktionen der Anwendungsprogrammierung. Und zu diesem Thema gibt es eine Menge Abbildungen.

Geschichte und Konzepte

2.1 Wie ein PC funktioniert

Nach heutigen Begriffen ist ein *Computer* ein elektronisches Gerät, das Berechnungen ausführen kann. Die gebräuchlichsten Typen nutzen spezielle Programmiersprachen, in denen *Programmierer* Anwendungen geschrieben haben und diese kompilieren, um bestimmte Aufgaben zu erledigen.

Die meisten Leute denken beim Begriff »Computer« ganz allgemein an computerartige Geräte, an Maschinen, die alle möglichen Dinge ausführen können. Auf einem typischen *Personal Computer* (PC) läuft das Betriebssystem Microsoft Windows und er erledigt die verschiedensten Aufgaben (Abbildung 2.2). Sie können beispielsweise Ihr Geld damit verwalten oder Computerspiele spielen, ohne dass irgendein zusätzlicher Aufwand erforderlich wäre, wie etwa das Hinzufügen neuer Hardware.



Abb. 2.2: Ein typischer PC

Hier ist eine Liste weiterer computerartiger Geräte, die allgemeinen Aufgaben dienen:

- Apple Mac
- Apple iPad
- Smartphone
- Laptop (Abbildung 2.3)



Abb. 2.3: Ein Laptop

Eine Menge anderer Geräte sind für ganz bestimmte Zwecke gedacht und konzentrieren sich auf eine einzige Aufgabe oder eine Reihe ähnlicher Aufgaben. Sie sind Ihnen vermutlich schon oft begegnet. Hier ist eine Liste gängiger spezialisierter, computerartiger Geräte:

- Taschenrechner
- Digitale Armbanduhr
- Digitaluhr
- Drahtloser Bilderrahmen (der per WLAN mit Daten versorgt wird)
- Einfaches Mobiltelefon
- Xbox One X
- GPS (*Global Positioning System*, das beispielsweise in Navigationsgeräten eingesetzt wird)
- Roku
- POS-System (*Point of sale*, automatisiertes Verkaufs- oder Kassensystem, siehe Abbildung 2.4)
- Digitalkamera



Abb. 2.4: POS-System in einer Zapfsäule

Die obige Liste ist nicht auch nur annähernd vollständig! Darüber hinaus gibt es Computer im *Inneren* von Myriaden anderer Geräte, wie z.B.:

- Moderne Kühlschränke
- Alle seit 1995 hergestellten Automobile
- Flugzeuge
- Schiffe und Boote
- Beleuchtungssysteme in Einkaufszentren
- Eisbearbeitungsmaschinen (Schlittschuhlaufen)
- Alarmanlagen

Sie verstehen schon, was gemeint ist: Computer halten die moderne Welt in Betrieb.

> **Hinweis**
>
> Ich habe mehr oder weniger willkürlich 1995 als das Jahr ausgewählt, ab dem in allen hergestellten Autos Computer vorhanden sind. Im Automobilbau werden jedoch schon länger Computer eingesetzt. Einfache Geräte fanden beispielsweise schon in den 1970er-Jahren in Autofabriken Verwendung. Der erste in Serie gefertigte Wagen mit einem zentralen Prozessor (zur Leistungsverbesserung), den ich gefunden habe, war ein BMW der 3er-Serie. Der BMW 325 aus den Jahren 1985 und 1986 konnte z.B. durch einen rund 200 € teuren Chip um einige PS aufgerüstet werden.

Moderne Computertechniker müssen die Funktionsweise all dieser Computertypen kennen, um Support für die vielen Geräte ihrer Kunden leisten zu können. Diese Gerätevielfalt spiegelt sich auch in den CompTIA A+-Prüfungen wider.

Falls Sie von der Vielzahl der Geräte eingeschüchtert sind, können Sie sich wieder entspannen. Sie brauchen als moderner Techniker nur zu wissen, dass die verschiedenen Geräte auf ganz ähnliche Weise funktionieren. Wenn Ihnen erst einmal bekannt ist, was ein bestimmtes Gerät für den Benutzer leisten soll, werden Sie auch in der Lage sein, das Gerät zu konfigurieren und Fehler zu beheben.

2.1.1 Bestandteile eines Computersystems

Zu einem modernen Computersystem gehören im Wesentlichen drei Bestandteile:

- Hardware
- Betriebssystem
- Anwendungen (Programme)

Zur *Hardware* gehören alle Objekte, die Sie anfassen oder in der Hand halten können. Im Falle eines Smartphones halten Sie beispielsweise das Telefon in der Hand. Und bei einem typischen Personal Computer berühren Sie beim Tippen die Tastatur oder betrachten Bilder auf dem Monitor.

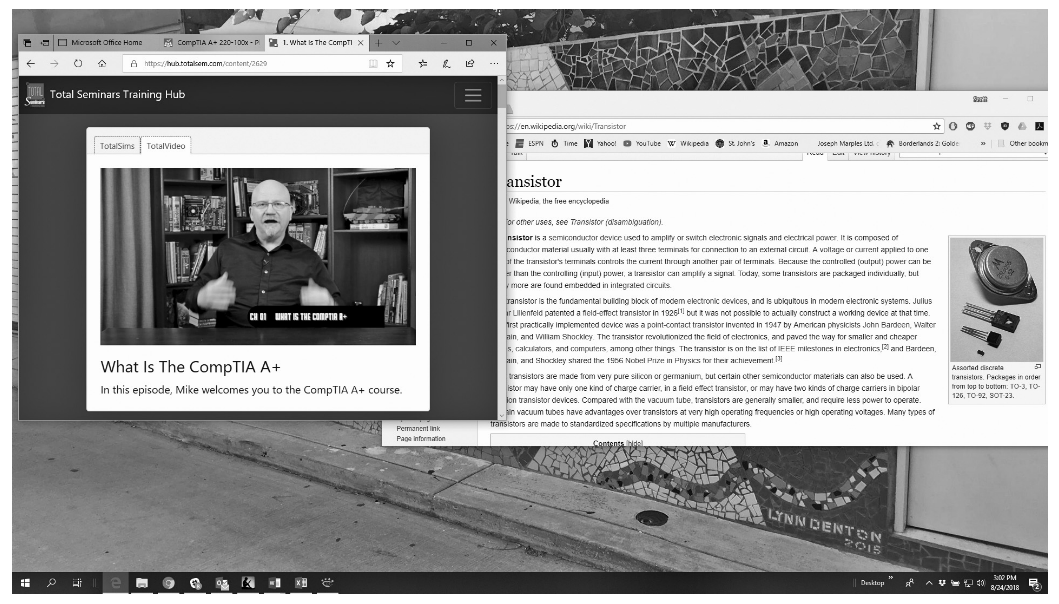


Abb. 2.5: Das Betriebssystem Microsoft Windows 10

Das *Betriebssystem* (*Operating System* oder kurz OS) steuert die Hardware und ermöglicht es Ihnen, dem Computer mitzuteilen, was er tun soll. Oftmals tritt das Betriebssystem als eine Ansammlung von Fenstern und kleinen Icons in Erscheinung, die Sie anklicken oder antippen können (Abbildung 2.5). Zusammengenommen wird das als Benutzeroberfläche oder *User Interface* (UI) bezeichnet. Damit sind die Teile der Software gemeint, mit denen Sie interagieren können. Ein UI, bei dem keine Befehle auf der Kommandozeile eingeben werden müssen, sondern stattdessen Symbole und Icons zur Auswahl anbietet, wird als *grafische Benutzeroberfläche* oder *Graphical User Interface* (GUI) bezeichnet.



Abb. 2.6: Einstellungen einer Digitalkamera ändern

Anwendungen (oder Programme) gestatten es Ihnen, bestimmte Aufgaben mit dem Computer zu erledigen, wie beispielsweise:

- Briefe zu schreiben
- Eine Nachricht von Ihrem Computer in Hamburg zum Computer Ihres Freundes in Rio de Janeiro zu übertragen
- Mit überall auf der Welt befindlichen anderen Leuten gemeinsam imaginäre Welten zu durchstreifen

Das Betriebssystem besonders einfacher computerartiger Geräte stellt womöglich nur einige wenige Funktionen zur Auswahl. So besitzt beispielsweise eine Digitalkamera ein Menü, das es erlaubt, Einstellungen vorzunehmen, wie etwa die Bildqualität der Aufnahmen (Abbildung 2.6).

Komplizierte Geräte bieten auch mehr Möglichkeiten. Ein Apple-iPhone beispielsweise kann schon im Auslieferungszustand eine ganze Menge cooler Sachen, nicht nur Anrufe tätigen. Außerdem können Sie den Apple-Onlinestore, den App Store, besuchen, sich dort nach weiteren Programmen umsehen und Anwendungen herunterladen (die als Apps bezeichnet werden), um alle möglichen Dinge zu machen, die Apple nicht mitliefert (Abbildung 2.7).

Und schließlich bieten Allzweckcomputer wie ein typischer Windows-PC oder ein Rechner mit macOS-Anwendungen, die Sie bei allem Möglichen unterstützen, vom Schreiben eines Buches über die CompTIA A+-Prüfungen bis hin zu einer Unterhaltung mit einer Person am anderen Ende der Welt, komplett mit Audio- und Videoübertragung (Abbildung 2.8).



Abb. 2.7: Das Spiel Monument Valley II aus dem Apple App Store



Abb. 2.8: Kommunizieren via Apple FaceTime

2.1.2 Ebenen eines Rechenvorgangs

Ganz grundsätzlich lassen sich bei der Funktionsweise eines Computers drei Ebenen unterscheiden. Man spricht hier auch von einem *Rechenvorgang*:

- Eingabe
- Verarbeitung
- Ausgabe

Zunächst einmal starten Sie den Vorgang, indem Sie irgendetwas unternehmen – mit der Maus klicken, auf der Tastatur etwas eintippen oder den Touchscreen berühren. Hierbei handelt es sich um die *Eingabe*. Zu diesem Zeitpunkt übernehmen die Bauteile im Inneren des Eingabegeräts oder im Gehäuse des Smartphones/Tablets, denn das Betriebssystem weist die Hardware an, die angeforderten Aktionen auszuführen. Dies ist die *Verarbeitung*.

Tatsächlich besitzt jedes computerartige Gerät letztendlich eine *zentrale Verarbeitungseinheit* (*Central Processing Unit*, CPU), die für gewöhnlich aus einer einzelnen, dünnen Siliziumscheibe und winzigen Transistoren besteht (Abbildung 2.9). Die CPU erledigt den Großteil der Verarbeitungsschritte und ist sozusagen das »Gehirn« des Computers.

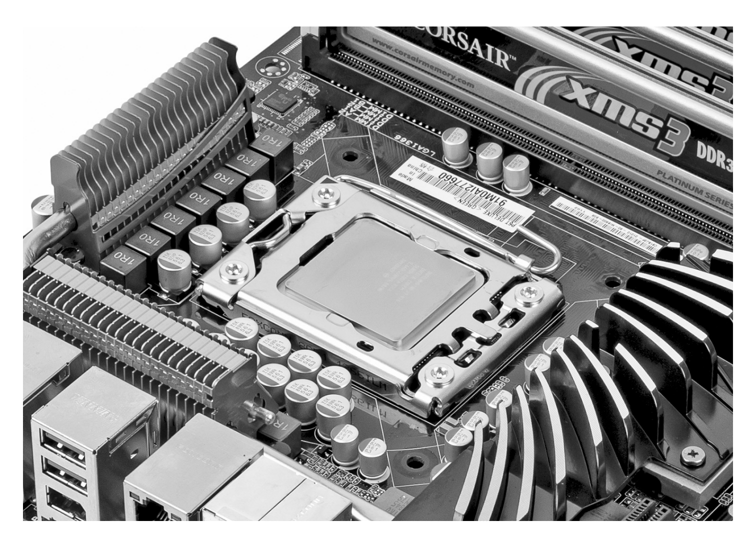


Abb. 2.9: Intel Core i7 CPU auf einem Mainboard

> **Hinweis**
>
> In Kapitel 3, *Mikroprozessoren*, erfahren Sie sehr viel mehr über CPUs und andere verarbeitende Komponenten.

Sobald der Computer Ihre Eingabe verarbeitet hat, zeigt er das Ergebnis an, indem er die Bildschirmanzeige ändert oder über die Lautsprecher Töne ausgibt. Hierbei handelt es sich um die *Ausgabe*. Ein Computer wäre nicht besonders nützlich, wenn er nicht anzeigen könnte, dass er Ihre Befehle ausgeführt hat! Abbildung 2.10 illustriert diesen Vorgang.

Bei modernen Computern kommen fast immer zwei weitere Ebenen hinzu:

- Datenspeicherung
- Netzwerkverbindung

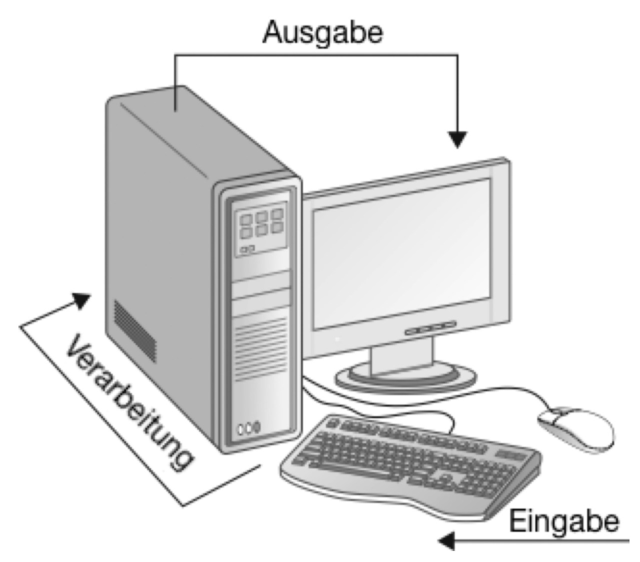


Abb. 2.10: Der Rechenvorgang

Bei der *Datenspeicherung* wird eine dauerhafte Kopie Ihrer Arbeit gesichert, damit Sie später weiter daran arbeiten können. Das Ganze funktioniert folgendermaßen: Zunächst einmal weisen Sie den Computer an, etwas abzuspeichern. Dann verarbeitet die CPU diesen Befehl und speichert die Daten ab. Abschließend zeigt der Computer irgendetwas an, etwa eine Meldung, die besagt, dass die Daten abgespeichert wurden. Wenn Sie Ihre Daten *nicht* abspeichern, gehen sie verloren, sobald Sie das Programm beenden oder den Computer ausschalten.

Die meisten Computer können sich mit anderen Geräten verbinden, um auf zusätzliche Ressourcen zuzugreifen. Für gewöhnlich wird eine Netzwerkverbindung genutzt, damit ein Computer mit einem oder mehreren anderen Computern Kontakt aufnehmen kann. Und das gilt nicht nur für die Computer am Arbeitsplatz. So kann sich jedes Smartphone mit dem Internet verbinden und beispielsweise Videos von YouTube abspielen (natürlich vorausgesetzt, dass Sie das Signal eines Funkmastes empfangen können und einen entsprechenden Datentarif gebucht haben).

An dieser Stelle werde ich häufig gefragt: »Wieso sollte ich mir über den Rechenvorgang Gedanken machen?« Die Antwort auf diese Frage macht einen guten Computertechniker aus. Hier ist sie.

2.1.3 Die Bedeutung des Rechenvorgangs für Techniker

Alle computerartigen Geräte führen Rechenvorgänge aus. Sie bilden daher die Grundlage dafür, wie ein Techniker solche Geräte zusammenbaut, aufrüstet und repariert. Die Kenntnis sowohl der beteiligten Komponenten als auch der Kommunikationsmethode ermöglicht es Ihnen, *jedes beliebige* Gerät zu verwenden. Vielleicht dauert es ein paar Minuten, um herauszufinden, wie man beispielsweise Eingaben an einem Gerät vornimmt, aber Sie werden den Bogen schnell heraushaben, wenn Sie die Funktionsweise der Geräte im Allgemeinen kennen.

2.1.4 Der Rechenvorgang im Detail

Der vollständige Vorgang besteht aus einer Menge einzelner Schritte und Teilen, die zusammenspielen müssen. Je besser Sie die Abläufe verstehen, umso leichter wird es Ihnen fallen, Fehler aufzuspüren, falls etwas schiefgeht. *Dies ist eine Grundregel für ausgezeichnete Techniker.*

Nachstehend finden Sie neun Schritte, die beim Erledigen einer Aufgabe für fast alle Computer und computerartigen Geräte gültig sind:

1. Einschalten – Computer benötigen Strom.
2. Die verarbeitenden Komponenten sind betriebsbereit.
3. Sie nehmen eine Eingabe vor.
4. Die verarbeitenden Komponenten bearbeiten Ihren Befehl.
5. Die verarbeitenden Komponenten geben Informationen auf den Ausgabegeräten aus.
6. Die Ausgabegeräte zeigen die Ergebnisse an.
7. Wiederholen Sie die Schritte 3 bis 6, bis Sie mit dem Resultat zufrieden sind.
8. Speichern Sie Ihre Arbeit ab.
9. Ausschalten des Computers.

Ich werde im weiteren Verlauf des Buches bei der Fehlersuche immer wieder auf diese Vorgehensweise zurückkommen. Denken Sie an diese Schritte, wenn Sie sich einem Problem gegenübersehen und die für Techniker entscheidende Frage stellen: Was könnte die Ursache sein? Oder etwas ausführlicher: Wodurch könnte das Problem verursacht werden, das ein reibungsloses Funktionieren des Geräts verhindert?

1001

2.2 Hardware

In weiten Teilen dieses Buches wird Ihnen ausführlich bestimmte Hardware vorgestellt, etwa CPUs und Massenspeichergeräte. Die CompTIA erwartet von kompetenten Technikern, dass sie die Bezeichnungen für Anschlüsse, Buchsen und Steckplätze einer Vielzahl verschiedener Geräte kennen. Anstatt sie hier alle kurz zu beschreiben, habe ich mich entschlossen, eine Fotostrecke zu erstellen, in der die wichtigsten Komponenten benannt werden. Außerdem finden Sie Verweise auf die Kapitel, in denen sie ausführlicher zur Sprache kommen.

Wichtig

Prägen Sie sich die Bezeichnungen der Komponenten und Anschlüsse sowie die in diesem Abschnitt genannten und erläuterten Begriffe gut ein. Sie werden Ihnen in den nachfolgenden Kapiteln, bei der praktischen Arbeit und in der CompTIA A+-Prüfung 1001 wieder begegnen.

Dieser Abschnitt soll Ihnen als eine visuelle Einführung in Komponenten und Anschlüsse dienen. Darüber hinaus sollte er auch hervorragend als Erinnerungsstütze für die Bezeichnungen bei der Vorbereitung auf die Prüfung 1001 geeignet sein. In den folgenden Abbildungen sind die Kapitel angegeben, in denen Sie weitere Informationen zu den Komponenten oder Standardanschlüssen finden.

Abbildung 2.11 zeigt einen typischen PC. Diese Ein- und Ausgabegeräte dürften den meisten Lesern bekannt sein.

Hinweis

Der Computer in Abbildung 2.11 ist ein Arbeitsplatzrechner, also ein Rechner, der an einem Schreibtisch benutzt wird. Im Gegensatz dazu dient ein *Server* dazu, Programme oder Speicherplatz über ein Netzwerk bereitzustellen. Wir kommen im Zusammenhang mit Netzwerken auf dieses Thema zurück.

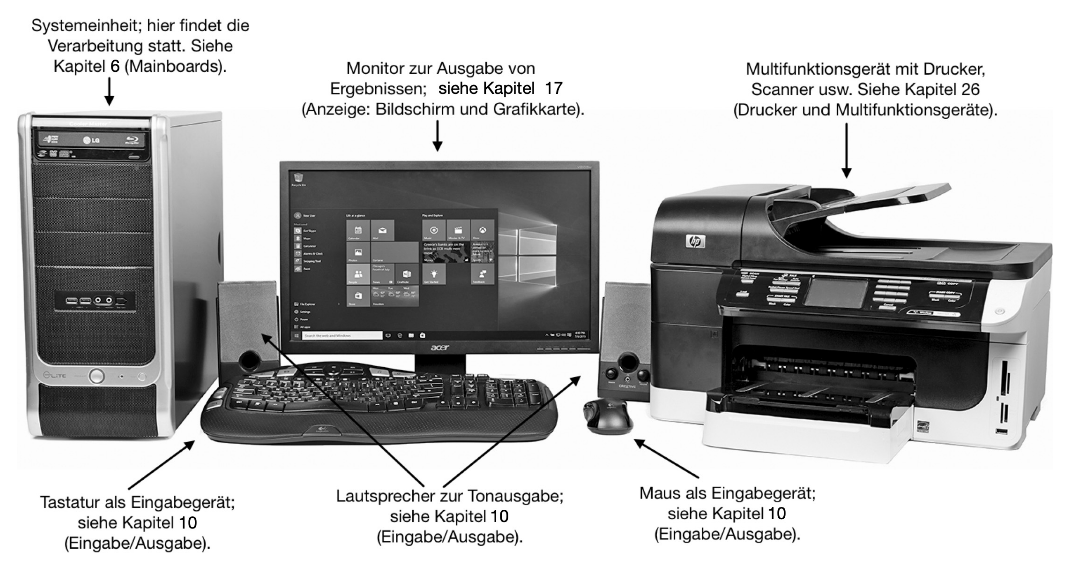


Abb. 2.11: PC mit gebräuchlichen Peripheriegeräten

Abbildung 2.12 zeigt die Rückseite der Systemeinheit eines PCs. Dort finden Sie viele Anschlüsse, die auch als *Ports* bezeichnet werden. An einigen davon werden Ausgabegeräte angeschlossen, andere hingegen dienen ausschließlich zum Anschließen von Eingabegeräten. Die meisten Anschlüsse können mit beiden Gerätetypen umgehen (wie etwa der *Universal Serial Bus* oder USB).

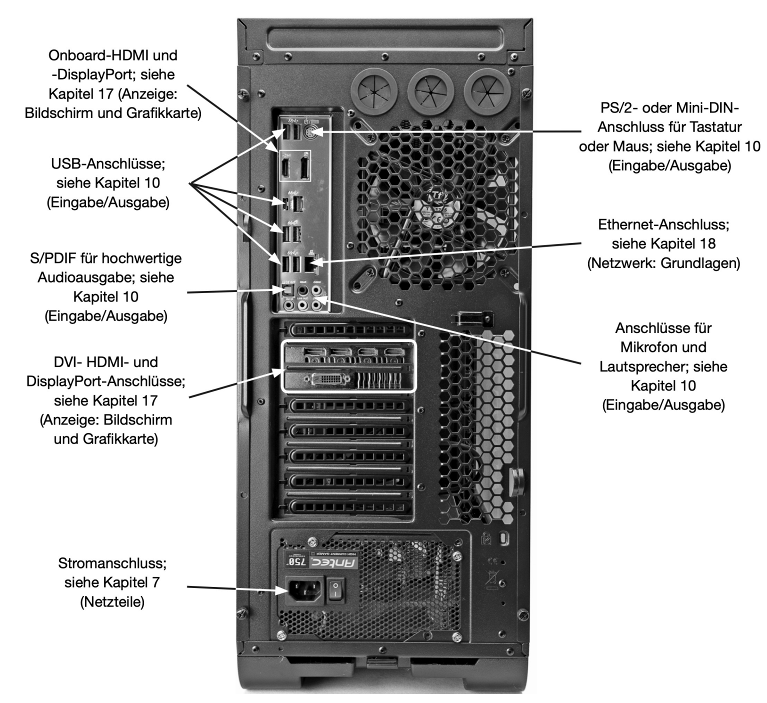


Abb. 2.12: Anschlüsse an der Rückseite eines PCs

Abbildung 2.13 zeigt das Innere eines PC-Gehäuses, in dem die verarbeitenden Komponenten und Speichergeräte zu finden sind. Unterhalb dieser Bauteile befindet sich das Mainboard, diejenige Komponente, mit der alle anderen direkt oder indirekt verbunden sind.

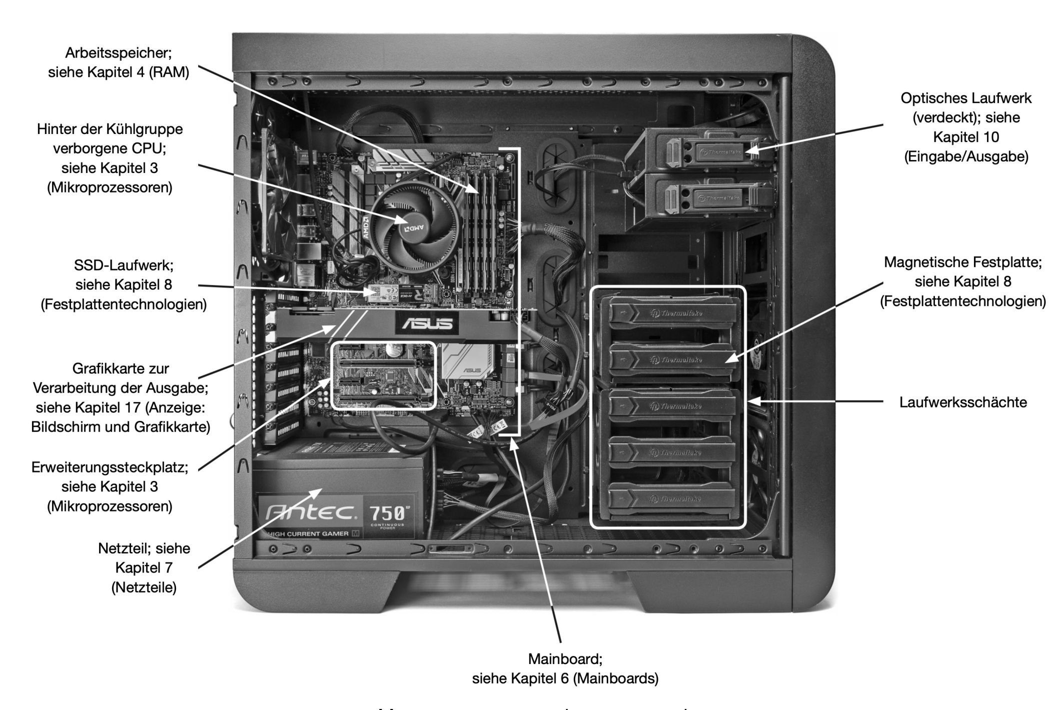


Abb. 2.13: Das Innere der Systemeinheit

Abbildung 2.14 zeigt einen zusammenklappbaren tragbaren Computer, hier ein Apple-MacBook-Air. Aufgrund der Portabilität des Geräts ist es wichtig, dass Ein- und Ausgabegeräte in das Gehäuse eingebaut sind. Deshalb handelt es sich hier um eine Variante des vorhin gezeigten typischen PCs, die Standardkomponenten sind hier aber ebenfalls vorhanden. In Kapitel 23, *Tragbare Computer*, werden wir einen eingehenden Blick auf die hier abgebildeten Komponenten werfen.

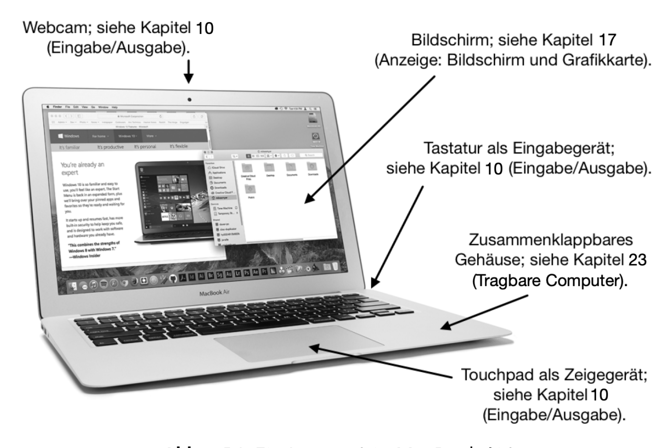


Abb. 2.14: Ein Laptop (ein MacBook Air)

In Abbildung 2.15 sehen Sie die Seite eines tragbaren Computers, auf der drei verschiedene Anschlüsse untergebracht sind.

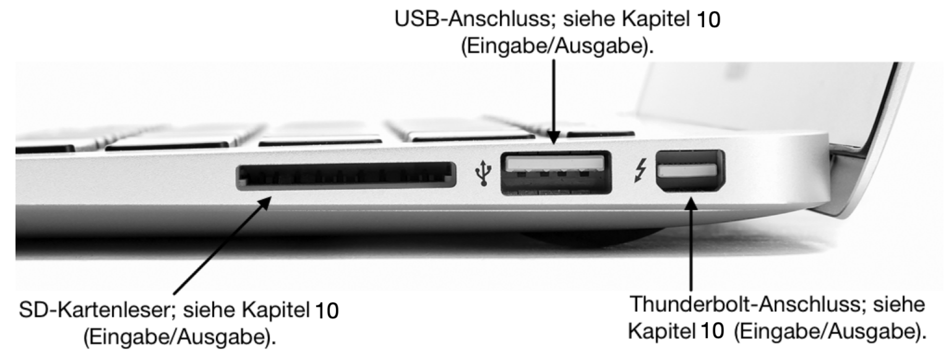


Abb. 2.15: Anschlüsse eines tragbaren Computers

Abbildung 2.16 zeigt einen Tablet-Computer, ein Apple-iPad. Beachten Sie hier, dass der Bildschirm berührungsempfindlich ist und auf diese Weise gleichzeitig als Ein- und Ausgabegerät dient.

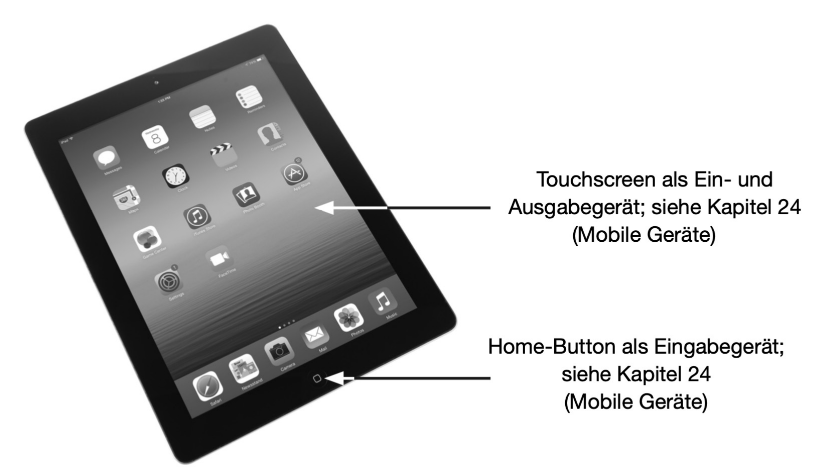


Abb. 2.16: Tablet-Computer

Ich könnte diese Fotostrecke noch mit einer Vielzahl weiterer Geräte fortsetzen, aber inzwischen sollte die Einheitlichkeit der Funktionsweise der Computerkomponenten ziemlich deutlich geworden sein. Sie arbeiten alle auf ähnliche Weise und als kompetenter Techniker sollten Sie in der Lage sein, für nahezu sämtliche Geräte Ihrer Kunden Support zu leisten. Sehen wir uns nun die Software an.

Tipp

Sehen Sie sich unbedingt die tolle Übung zu Kapitel 2 unter `http://totalsem.com/100x` an, bei der den Anschlüssen des Mainboards die richtigen Bezeichnungen zugeordnet werden müssen. Diese coole Simulation erleichtert es, sich die Namen der Anschlüsse zu merken.

1002

2.3 Software

Die CompTIA A+-Prüfung 1002 hat eine Menge Software zum Inhalt, allerdings geht es dabei vornehmlich um Dienstprogramme des Betriebssystems und weniger um bestimmte Anwendungen. Den Großteil machen die drei Betriebssysteme Microsoft Windows, Apple Macintosh OS und Linux aus. Die Prüfung deckt Windows 7, Windows 8, Windows 8.1 und Windows 10 ab. Das aktuelle Betriebssystem von Apple heißt macOS – so wird es in diesem Buch bezeichnet. Die Prüfung deckt Linux allgemein ab, aber keine Distributions-spezifischen Features. Das Buch folgt dem gleichen Muster.

Wichtig

In den Lernzielen wird das Apple-Betriebssystem für Arbeitsplatzrechner als »Apple Macintosh OS« oder als »Mac OS« bezeichnet. Apple hat den Namen allerdings 2016 geändert: »Mac OS X« heißt jetzt »macOS«. Mit all diesen Bezeichnungen ist das gleiche Betriebssystem gemeint.

Neben den Betriebssystemen für Arbeitsplatzrechner deckt die CompTIA A+-Prüfung 1002 auch vier Betriebssysteme für Smartphones/Tablets ab: Microsoft Windows, Google Android, Apple iOS und Google Chrome OS. Mit 98 Prozent Marktanteil sind Android und iOS vorherrschend. Windows und Chrome OS sind bestenfalls Außenseiter.

2.3.1 Gemeinsame Funktionalitäten verschiedener Betriebssysteme

Die verschiedenen Betriebssysteme unterscheiden sich natürlich, bestimmte Funktionen sind ihnen jedoch gemeinsam:

- Das Betriebssystem kommuniziert mit der Hardware des PCs oder des Geräts oder stellt anderen Programmen eine solche Kommunikationsmethode zur Verfügung. Jedes Betriebssystem benötigt spezielle Hardware. So müssen Sie auf einem Computer mit 32-Bit-CPU beispielsweise die 32-Bit-Version eines Betriebssystems installieren. Für einen Computer mit 64-Bit-CPU ist hingegen ein 64-Bit-Betriebssystem erforderlich.
- Das Betriebssystem stellt eine Benutzeroberfläche bereit – eine visuelle Abbildung des Computers, die für die Benutzer des Geräts einen Sinn ergibt.
- Das Betriebssystem erlaubt es den Benutzern, festzustellen, welche installierten Anwendungen verfügbar sind, und Programme ihrer Wahl zu starten, zu nutzen und zu beenden.
- Das Betriebssystem ermöglicht es den Benutzern, Programme und Daten hinzuzufügen, zu verschieben und zu löschen.
- Das Betriebssystem stellt eine Methode zur Verfügung, um das System vor allen möglichen Bedrohungen zu schützen, beispielsweise vor Datenverlust oder unerlaubtem Zugriff.

Alle Betriebssysteme ermöglichen es Ihnen, Programme auszuführen, allerdings sind die Formate so unterschiedlich, dass nicht jedes Programm auf jedem Betriebssystem installiert werden kann. Programmierer müssen zusätzliche Arbeit leisten, um eigene Versionen von Programmen für verschiedene Betriebssysteme zu erstellen. In der CompTIA A+-Prüfung 1002 ist hier von der *Betriebssystemkompatibiltät* die Rede. Die Software, die Ihre Benutzer verwenden, kann die Auswahl der möglichen Betriebssysteme einschränken. Darüber hinaus kann sie Auswirkungen darauf haben, wie gut Benutzer verschiedener Betriebssysteme miteinander zusammenarbeiten können!

Ein weiteres Kompatibilitätsproblem ergibt sich, wenn ein Betriebssystem mit einer bestimmten Hardware nicht kommunizieren kann. Ein Gerät, das mit einem Betriebssystem gut funktioniert, könnte mit einem anderen Betriebssystem nur mangelhaft oder gar nicht funktionieren. Ein bestimmtes Betriebssystem benötigt möglicherweise keine zusätzliche Software, um ein Gerät zu verwenden, für ein anderes hingegen könnte ein spezielles Programm zu seiner Ansteuerung erforderlich sein. Und

brandneue Hardware funktioniert manchmal erst dann vernünftig, wenn das Betriebssystem eine Aktualisierung erhält, die die neue Hardware unterstützt.

In fast allen Kapiteln dieses Buches geht es um das Zusammenspiel von Betriebssystem und Hardware. Kapitel 11, *Der maßgeschneiderte PC*, befasst sich mit der Installation und dem Entfernen von Programmen. Sicherheitsaspekte kommen in mehreren Kapiteln vor, etwa in Kapitel 13, *Benutzer, Gruppen und Berechtigungen*, und in Kapitel 27, *Computersicherheit*. Der verbleibende Teil dieses Kapitels konzentriert sich daher auf Benutzeroberflächen und Dateistrukturen.

2.3.2 Benutzeroberflächen

Dieser Abschnitt stellt die Benutzeroberflächen der verschiedenen Betriebssysteme vor. Er soll, wie schon die Hardware-Fotostrecke, zwei Aufgaben erfüllen. Zum einen müssen Sie die korrekten Bezeichnungen für die vielen Funktionalitäten der Benutzeroberfläche kennen und deren Funktionsweise verstehen. Zum anderen dient er als praktischer Abschnitt zum Nachschlagen, bevor Sie die CompTIA A+-Prüfung 1002 ablegen.

Hinweis

In Kapitel 24, *Mobile Geräte*, werden die Betriebssysteme für mobile Geräte (iOS, Android, Windows und Chrome OS) eingehend betrachtet.

Windows 7

Abbildung 2.17 zeigt die Standardansicht für Windows 7, einem herkömmlichen Allzweckbetriebssystem. Windows verwendet vornehmlich eine grafische Benutzeroberfläche. Sie verwenden also eine Maus oder ein anderes Zeigegerät, um Bedienelemente anzuklicken. Der Hintergrund wird als *Desktop* bezeichnet. Bei den geöffneten Programmen handelt es sich um den Internet Explorer – den Standard-Webbrowser in Windows 7 – und ein Fenster des Windows-Explorers, der die vier Standardbibliotheken von Windows 7 anzeigt.

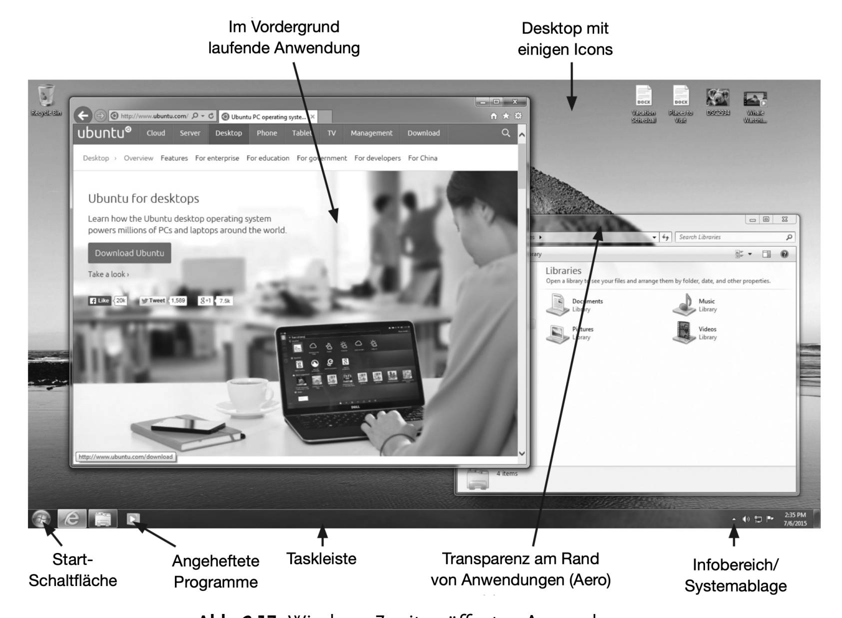


Abb. 2.17: Windows 7 mit geöffneten Anwendungen

Die anderen sichtbaren Objekte haben folgende Bedeutung:

- Die geöffneten Anwendungen demonstrieren die *Transparenz*, bei der durch die Ränder der Anwendungsfenster Hintergrundbilder verschwommen sichtbar sind. Diese Funktion wird als *Aero* oder *Aero-Desktop* bezeichnet.
- Klicken Sie auf die START-Schaltfläche, um auf Anwendungen, Dienstprogramme, Dateien und Ordner zuzugreifen.
- *Angeheftete Programme* können mit einem einzelnen Linksklick gestartet werden.
- Die *Taskleiste* zeigt laufende Programme an.
- Der *Infobereich* zeigt im Hintergrund laufende Programme an. Viele Techniker verwenden auch die Bezeichnung *Systemablage*.

Die Bedienung der klassischen Windows-Benutzeroberfläche erfolgt größtenteils durch die Verwendung einer Maus oder eines Touchpads, um den Mauszeiger zu bewegen und Links- oder Rechtsklick auf die Icons auszuführen. Ein einfacher Linksklick wählt ein Objekt aus, ein doppelter öffnet es. Ein Rechtsklick öffnet ein *Kontextmenü*, das verschiedene Optionen zur Auswahl stellt (Abbildung 2.18).

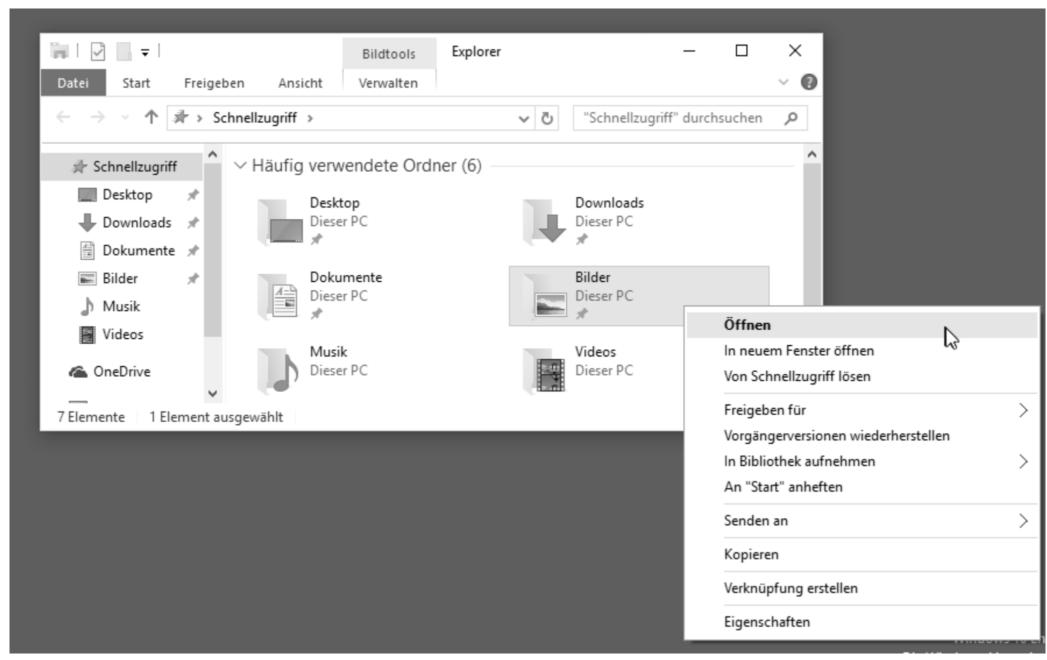


Abb. 2.18: Kontextmenü

> **Hinweis**
>
> Das Kontextmenü bietet Optionen an, die von dem Objekt abhängig sind, das Sie rechtsklicken. Das durch den Rechtsklick auf eine Datei angezeigte Kontextmenü unterscheidet sich beispielsweise erheblich von dem Kontextmenü, das nach einem Rechtsklick auf ein Programm erscheint.

Windows 8/8.1

Mit der Vorstellung von Windows 8 nahm Microsoft signifikante Änderungen an der Windows-Benutzeroberfläche vor. So wurden Anleihen bei Tablet-Betriebssystemen wie Windows Phone gemacht und sogenannte *Kacheln* für Programme im Vollbildmodus eingeführt, die als Apps bezeichnet werden.

Beachten Sie hier, dass auf dem Bildschirm die *angehefteten Apps*, die vom Benutzer ausgewählten Standardprogramme angezeigt werden – nicht sämtliche auf dem Computer installierten Programme.

Die Windows-8-Bedienoberfläche erhielt den Codenamen *Metro UI* und ist besonders gut für Geräte mit berührungsempfindlichen Bildschirmen geeignet, die durch Touchgesten bedient werden. Der PC wird praktisch zu einem riesigen Tablet. Tippen Sie auf eine App, um sie zu starten, oder streichen Sie mit dem Finger über den Bildschirm, um weitere Apps anzuzeigen – das macht wirklich Spaß! Abbildung 2.19 zeigt die Standardansicht von Windows 8, den Startbildschirm, auf dem einige Bedienelemente gekennzeichnet sind.

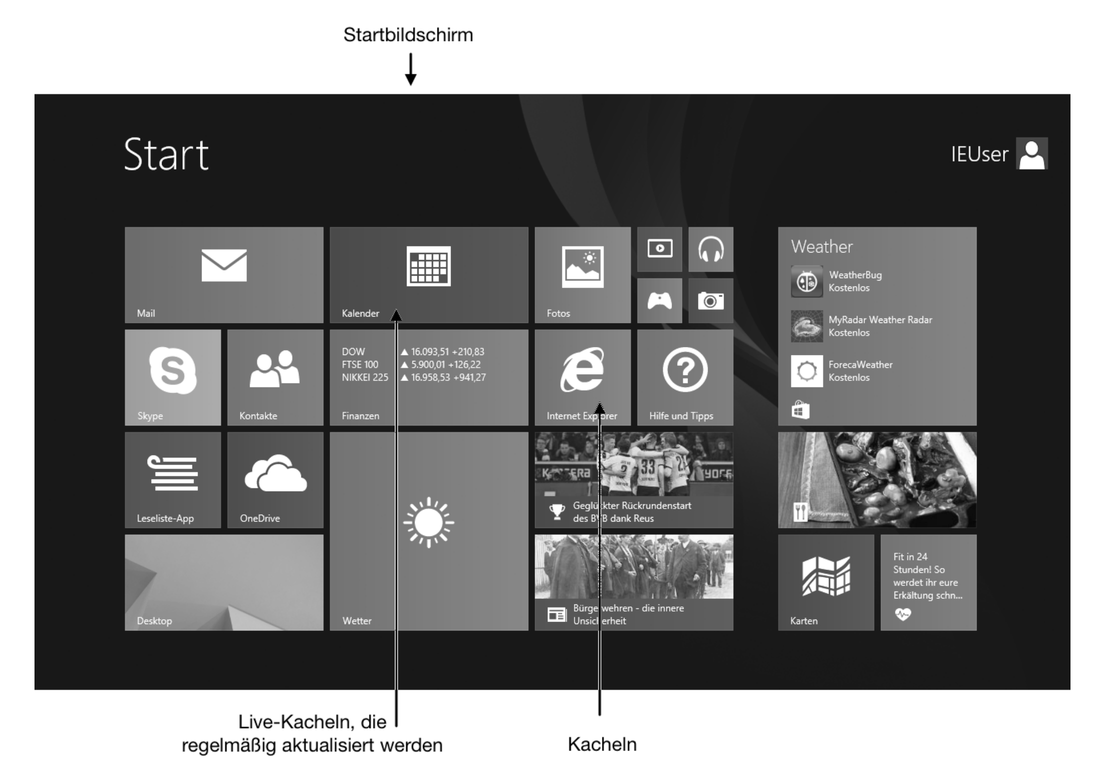


Abb. 2.19: Der Startbildschirm von Windows 8

> **Hinweis**
>
> Den Spitznamen »Metro UI« hat Microsoft kurz vor der Veröffentlichung von Windows 8 aus rechtlichen Gründen verworfen und durch »Modern UI« ersetzt. Viele Techniker und IT-Profis bezeichnen die Kacheloberfläche von Windows 8/8.1 aber nach wie vor als »Metro«.

Windows 8 besitzt auch einen klassischen Desktop, bei dem auffällt, dass es keine sichtbare START-Schaltfläche mehr gibt (Abbildung 2.20). Sie können durch Drücken der Windows-Taste auf einer Standardtastatur auf diesen Desktop zugreifen.

Die Bedienung mit Tastatur und Maus hat vielen Benutzern zu schaffen gemacht und sie davon abgehalten, von Windows 7 auf Windows 8 zu wechseln. Beispielsweise scrollt die Betätigung des Scrollrads den Bildschirm nicht hoch und runter, sondern nach links und rechts (Abbildung 2.21).



Abb. 2.20: Der Desktop von Windows 8

Windows 8 macht sich mit dem Feature *Fenster nebeneinander anzeigen* moderne Breitbildschirme zunutze. Wenn Sie eine Anwendung auswählen und dann die Windows-Taste und den Pfeil nach links drücken, wird die Anwendung an der linken Seite des Bildschirms angeheftet. Wenn Sie das mit einer weiteren Anwendung wiederholen, wird diese an der rechten Hälfte des Bildschirms angeheftet. In Programmen wie Microsoft Word, die für jedes Dokument ein eigenes Fenster öffnen, ist es so sehr einfach, zwei Dokumente miteinander zu vergleichen.



Abb. 2.21: Der nach rechts gescrollte Startbildschirm von Windows 8

Hinweis

Der Windows Store (Windows 7/8.x) oder der Microsoft Store (Windows 10) ermöglichen es, Apps direkt bei Microsoft zu kaufen. Die dafür zuständige App heißt STORE, Microsoft hat den Store mehrfach aktualisiert, um beispielsweise das Xbox-Spiel-System einzubinden. Darüber hinaus sind im Store vor allem Touch-First-Apps erhältlich, also Programme, bei denen die Bedienbarkeit mit einem Touchscreen besonders berücksichtigt wird.

Mit einer Reihe von Updates, die mit Windows 8.1 ihren Abschluss fand, hat Microsoft bekannte Funktionalitäten wieder zurückgebracht, beispielsweise die START-Schaltfläche, einfachen Zugriff auf eine Schaltfläche zum Schließen von Programmen und die Möglichkeit, direkt mit dem Desktop zu starten. Abbildung 2.22 zeigt die Standardansicht von Windows 8.1 mit einigen markierten Bedienelementen. Beachten Sie die Ähnlichkeit zu Windows 7.

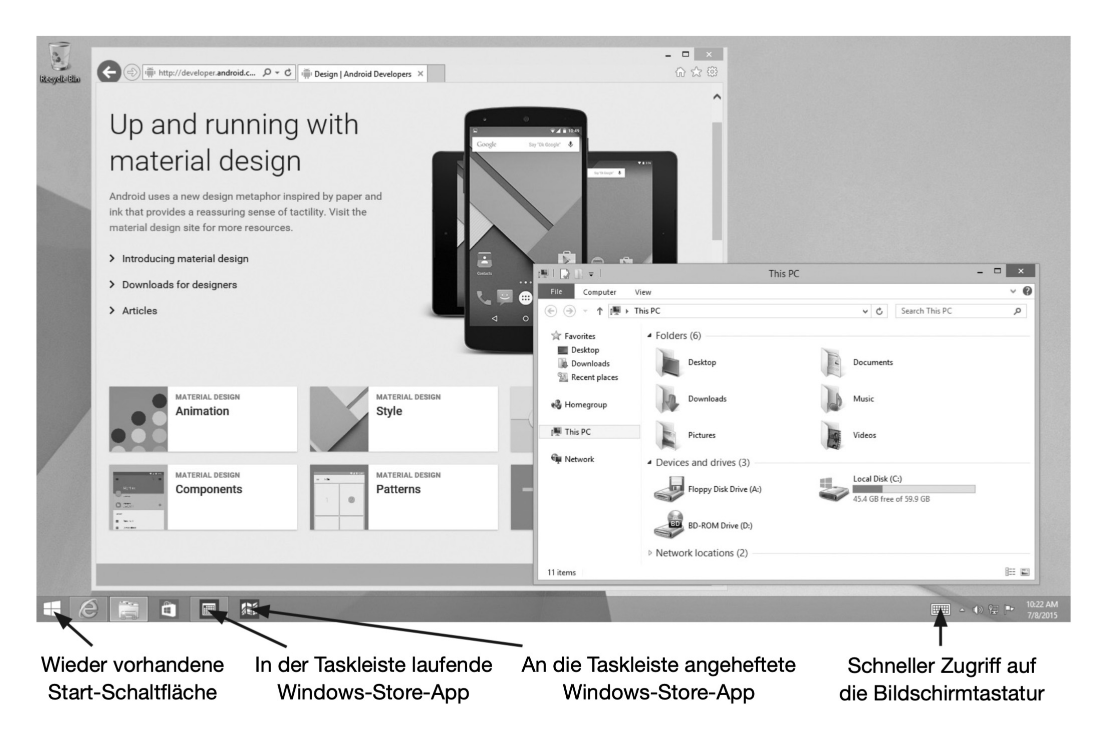


Abb. 2.22: Windows 8.1

In Windows 8.1 ist es sehr einfach, Apps an den Startbildschirm anzuheften. Die Anwahl des Pfeils unten links zeigt die Apps und Dienstprogramme an, die Sie dann sortieren und auswählen können (Abbildung 2.23). Rechtsklicken Sie auf ein Icon, um es am Startbildschirm anzuheften.

Windows 8/8.1 enthält viele versteckte Bedienelemente, die aktiviert werden, wenn Sie den Mauszeiger an einer bestimmten Stelle des Bildschirms platzieren. Wenn Sie den Mauszeiger beispielsweise in die linke untere Ecke des Startbildschirms bewegen, wird die Start-Schaltfläche aktiviert (Abbildung 2.24).

Wichtig

In der ersten Version von Windows 8 gab es auf dem Desktop keine sichtbare START-Schaltfläche (von der Charm-Leiste mal abgesehen). Microsoft hat sie mit einer späteren Aktualisierung wieder hinzugefügt.

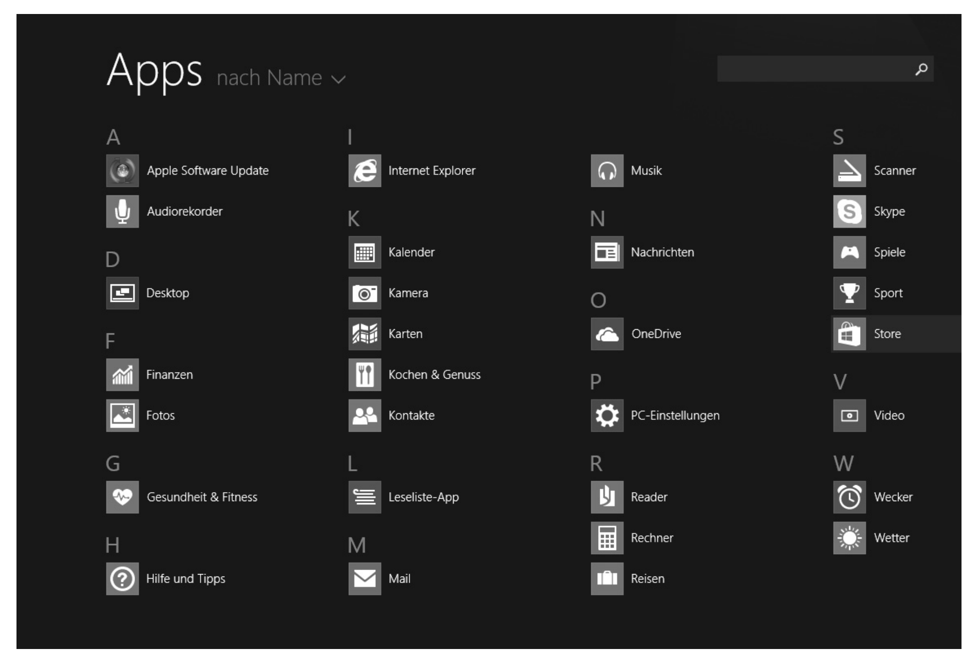


Abb. 2.23: Nach Namen sortierte Apps



Abb. 2.24: Wie von Zauberhand erscheint die START-Schaltfläche

Wenn Sie den Mauszeiger in der oberen oder unteren rechten Bildschirmecke positionieren, wird die Charm-Leiste angezeigt. Werfen Sie einen Blick auf die rechte Seite der Abbildung 2.25. Zu den Charms gehört ein praktisches Suchwerkzeug, das es erlaubt, von einer Stelle aus den Computer oder sogar das Internet zu durchsuchen. Mit dem Charm TEILEN können Sie Fotos, Nachrichten usw. mit anderen teilen. Ich komme später in diesem Kapitel wieder auf die Charms zurück, wenn wir uns damit befassen, wie man auf die Dienstprogramme zugreift.



Abb. 2.25: Zugriff auf die Charms durch Positionieren der Maus in der oberen oder unteren rechten Ecke

Die endgültige Version von Windows 8.1 verwendet den Desktop als Standardansicht, nicht den Startbildschirm. Die START-Schaltfläche wird unten links angezeigt (Abbildung 2.26). Auf die Charms können Sie nach wie vor zugreifen, indem Sie den Mauszeiger in der oberen oder unteren rechten Bildschirmecke platzieren.

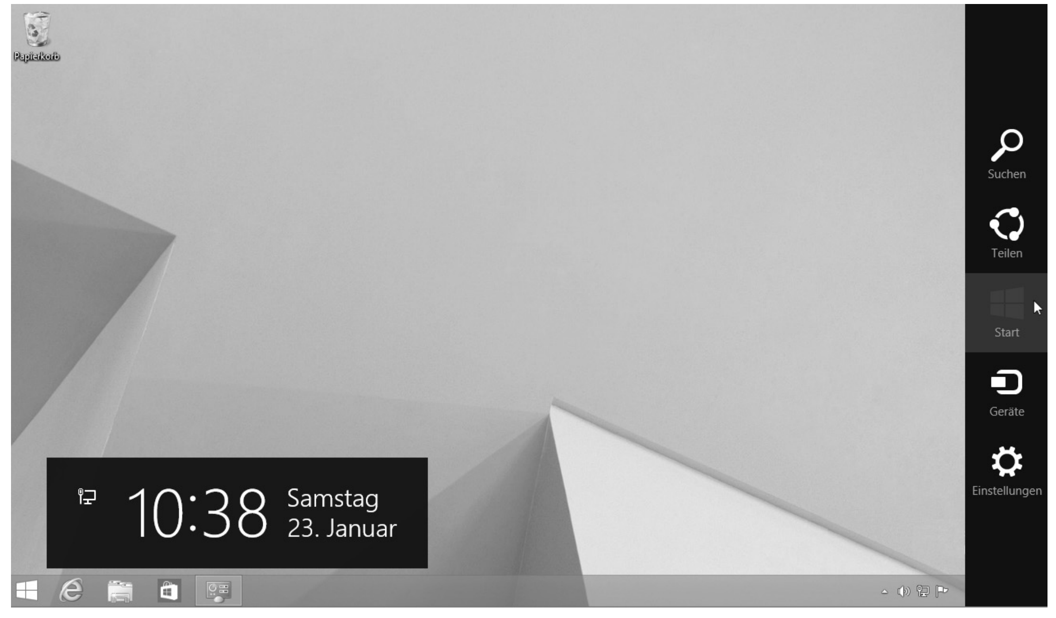


Abb. 2.26: Der Desktop von Windows 8.1

Wichtig

Windows 8 bietet interessante Optionen in der Taskleiste, wenn man mehrere Bildschirme verwendet. Standardmäßig werden laufende und angeheftete Anwendungen sowohl auf dem Hauptbildschirm als auch auf weiteren Bildschirmen dargestellt. Die Taskleiste kann auch Icons für Programme anzeigen, die auf einem bestimmten Bildschirm laufen. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie EIGENSCHAFTEN, um das Verhalten zu ändern.

Windows 10

Mit Windows 10 hat Microsoft ein Betriebssystem entwickelt, das dem herkömmlichen Windows 7 einige der fortschrittlicheren Features des Metro/Modern UI von Windows 8.x beimengt. Microsoft hat insbesondere aus Überzeugung die START-Schaltfläche zurückgebracht und die nicht gerade beliebte Charm-Leiste entfernt. Die wichtigsten Tools – ich verwende z.B. die Suche ständig –, hat Microsoft nun in die linke untere Ecke des Desktops in der Taskleiste integriert. Abbildung 2.27 zeigt die Oberfläche von Windows 10 mit einer aktiven Anwendung im Vordergrund.

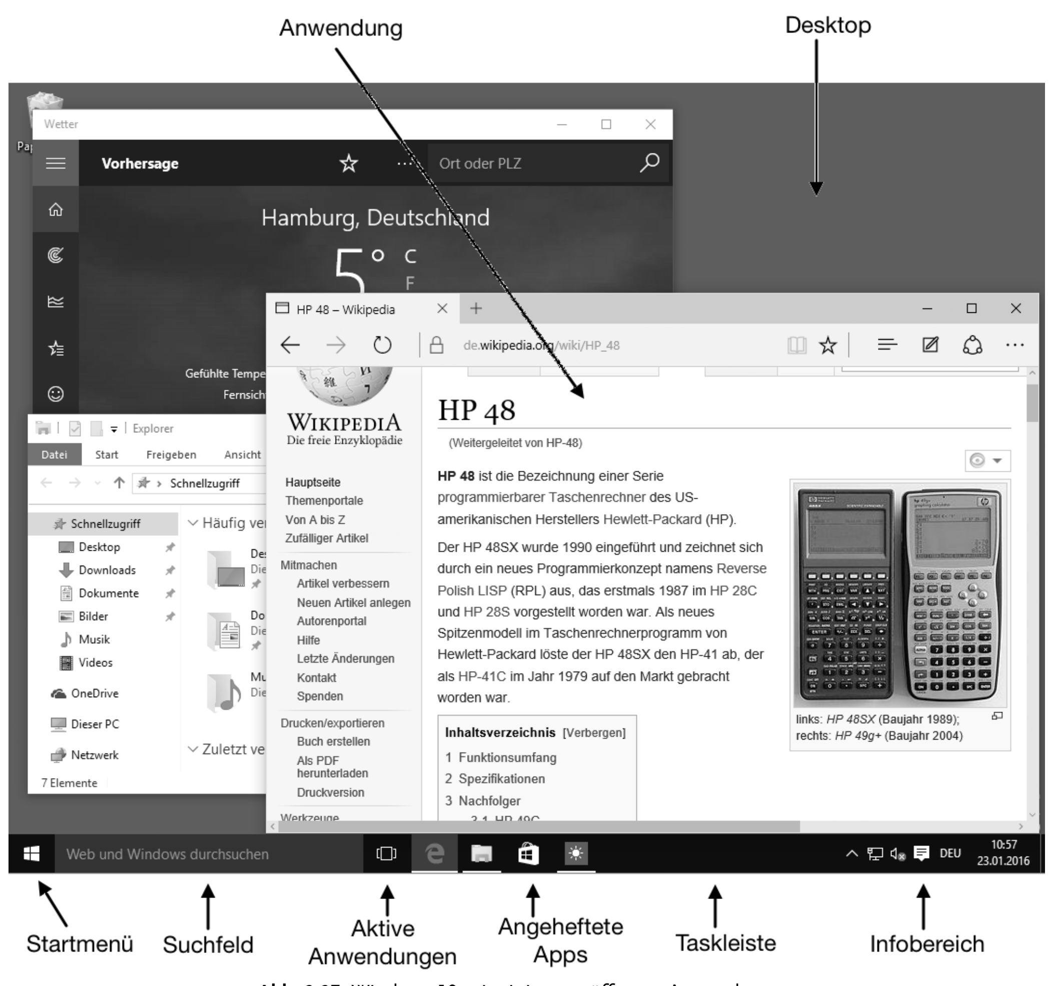


Abb. 2.27: Windows 10 mit einigen geöffneten Anwendungen

Wenn Sie auf der Tastatur die Windows-Taste betätigen, zeigt Windows 10 das Startmenü an, das auf der linken Seite nützliche Werkzeuge und die am häufigsten verwendeten Apps und auf der rechten Seite die angehefteten Apps enthält (Abbildung 2.28). Wie in Windows 8.1 können Sie mit einem Klick auf den sinnvollerweise ALLE APPS benannten Link (unten links) eine Liste aller installierten Programme öffnen. Klicken Sie eine App mit der rechten Maustaste an, um sie am Startbildschirm anzuheften.

Hinweis

Windows 10 verfügt außerdem über einen Tablet-Modus, der so wie der Bildschirm mit Kacheln in Windows 8 (8.1) aussieht. Dieser Modus erweist sich bei berührungsempfindlichen Geräten als äußerst nützlich.

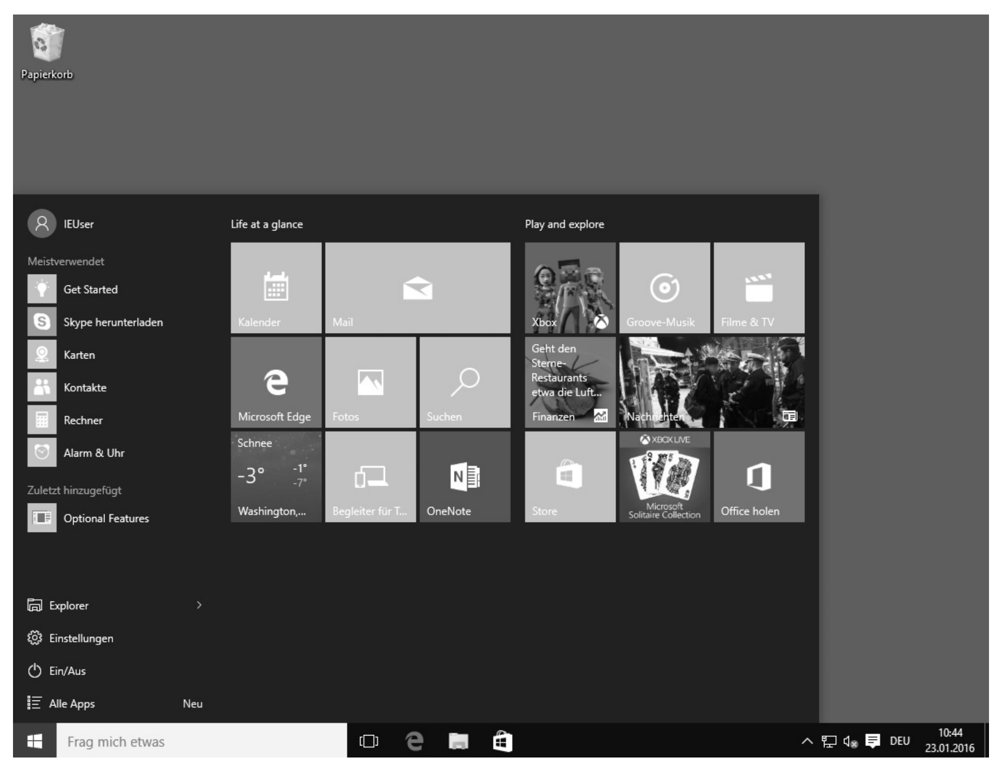


Abb. 2.28: Das Startmenü in Windows 10

Klicken Sie auf die Schaltfläche AKTIVE ANWENDUNGEN, um mehrere Desktops zu verwalten und die geöffneten Anwendungen zu gruppieren. macOS und Linux verfolgen bei dieser Funktionalität eigene Ansätze, wie Sie in den nächsten Abschnitten sehen werden.

Hinweis

In Windows 10 wurde das in Windows 8 eingeführte Nebeneinanderausführen von Apps geändert. Drücken Sie die [Win]-Taste und die [→]- bzw. die [←]-Taste, um das Fenster einer Anwendung auf einer Seite des Bildschirms anzudocken. Außerdem werden auf der gegenüberliegenden Bildschirmseite Icons der anderen laufenden Programme angezeigt. Wenn Sie auf eines der Icons klicken, nimmt das fragliche Programm die andere Bildschirmhälfte ein.

macOS

Die Benutzeroberfläche des Betriebssystems macOS bietet ähnliche Funktionen wie Windows. Der Hintergrund des Hauptbildschirms heißt *Schreibtisch*. Auf häufig genutzte Anwendungen können Sie durch einen Klick auf die Programmsymbole im *Dock* zugreifen, der Leiste, die sich standardmäßig am unteren Ende des Bildschirms befindet. Per Drag-and-drop können dem Dock Programme hinzugefügt werden, und wie bei angehefteten Apps lassen sie sich mit einem Rechtsklick wieder entfernen. Das Dock leistet jedoch noch mehr: Es zeigt auch (wie die Taskleiste in Windows) die laufenden Programme an. Abbildung 2.29 zeigt eine typische Ansicht der Oberfläche von macOS.



Abb. 2.29: macOS

Auf Apple-Tastaturen gibt es eine spezielle Taste (Abbildung 2.30) zum Aufruf von *Mission Control*, das alle geöffneten Fenster in einer übersichtlichen Darstellung anzeigt und es Ihnen erlaubt, in andere geöffnete Anwendungen zu wechseln (Abbildung 2.31). Sie können Mission Control auch durch gleichzeitiges Drücken von `Strg` und `↑` aufrufen.



Abb. 2.30: Die Taste zum Aufruf von Mission Control

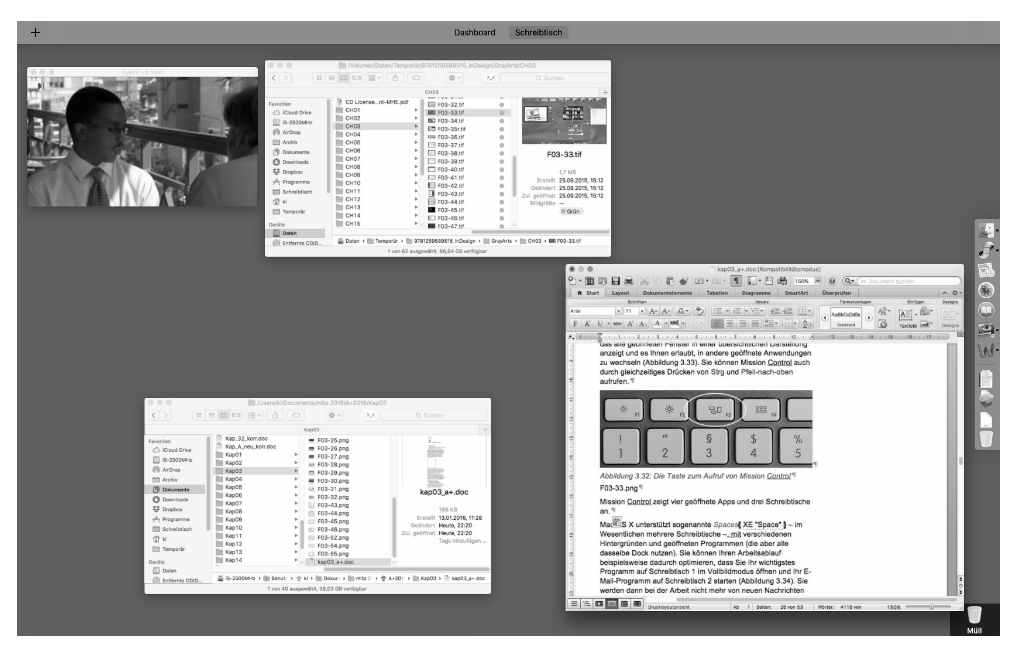


Abb. 2.31: Mission Control zeigt vier geöffnete Fenster und zwei Schreibtische an.

macOS unterstützt sogenannte *Spaces* – im Wesentlichen mehrere Schreibtische –, mit verschiedenen Hintergründen und geöffneten Programmen (die aber alle dasselbe Dock nutzen). Sie können Ihren Arbeitsablauf beispielsweise dadurch optimieren, dass Sie Ihr wichtigstes Programm auf Schreibtisch 1 im Vollbildmodus öffnen und Ihr E-Mail-Programm auf Schreibtisch 2 starten (Abbildung 2.32).



Abb. 2.32: Von einem Schreibtisch zum nächsten wechseln

Sie werden dann bei der Arbeit nicht mehr von neuen Nachrichten unterbrochen, können bei Bedarf jedoch leicht mittels Mission Control auf den zweiten Schreibtisch zugreifen. In den jüngsten Versionen von macOS können Sie bei gedrückter `Strg`-Taste mit den Tasten `←` und `→` durch die Spaces navigieren.

Wichtig

In Windows 10 können Sie mit »Aktive Anwendungen« mehrere Desktops nutzen. Ältere Windows-Versionen unterstützen diese Funktion jedoch nicht.

Linux

Die vielen verschiedenen Linux-Distributionen bieten eine große Vielfalt an Benutzeroberflächen, die als *Desktop-Umgebungen* bezeichnet werden. Sie verfügen über ähnliche Funktionen wie Windows oder macOS. Abbildung 2.33 zeigt eine weitverbreitete Linux-Distribution, nämlich Ubuntu Linux mit dem GNOME-Desktop. Die verschiedenen Funktionalitäten sind in der Abbildung gekennzeichnet. Häufig genutzte Dienstprogramme und Anwendungen können in der Startleiste am linken Bildschirmrand gesichert werden. Die meisten Distributionen bieten Optionen zum Surfen im Internet, E-Mail, Zugriff auf Ordner und Dateien und so weiter.

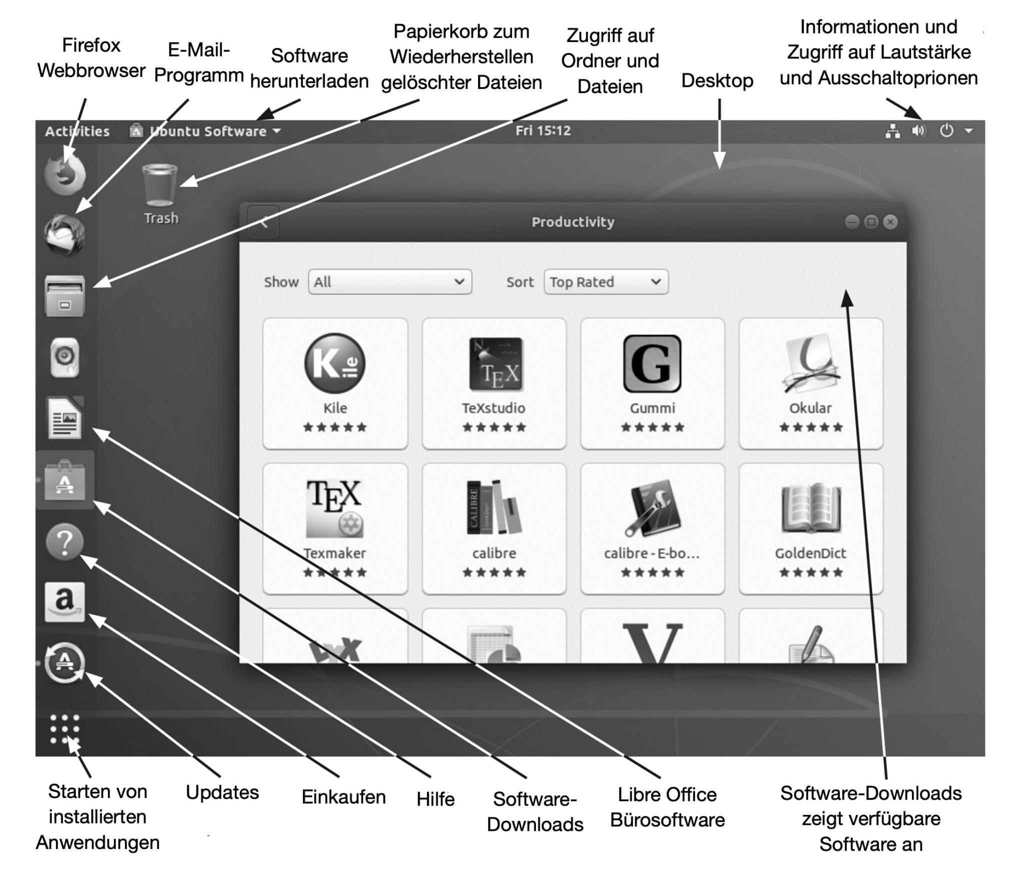


Abb. 2.33: Ubuntu Linux

Tipp

Unter `Ubuntu.com` steht ein schon recht stabiler Emulator für Ubuntu Linux bereit, der es ermöglicht, mit dem Desktop herumzuexperimentieren, Einstellungen auszuprobieren usw. Probieren Sie es aus! Besuchen Sie `http://tour.ubuntu.com` und testen Sie das System.

2.3.3 Dateistrukturen und Pfade

Zu wissen, wo sich bestimmte Inhalte befinden (Dateien und die Ordner, in denen sie enthalten sind), ist für Techniker sehr nützlich, wenn Sie den Benutzern helfen möchten, ihr tägliches Arbeitspensum effizienter zu erledigen. Nahezu jedes Betriebssystem speichert Dateien in Ordnern, die eine Baumstruktur bilden. Die Pfadbezeichnung beginnt mit dem Laufwerk oder dem Speichermedium, der Wurzel dieses Baums. Ihm folgen die Namen des Ordners, Unterordners, Unterunterordners usw., bis man zur gewünschten Datei gelangt. Das Laufwerk oder Speichermedium erhält eine Bezeichnung, für gewöhnlich einen *Laufwerksbuchstaben* wie `C:`. In Kapitel 9, *Vorbereitung und Wartung von Festplatten*, werden wir gründlich untersuchen, welche Methoden zur Datenspeicherung moderne Betriebssysteme einsetzen. Dieser Abschnitt widmet sich mehr der Besessenheit der CompTIA, von den Prüflingen zu verlangen, Pfade auswendig zu lernen.

Windows

In Windows gibt es eine Reihe wichtiger Ordner, die dabei helfen, Ihre Programme und Dokumente zu organisieren. Sie befinden sich in einem Verzeichnis, das als *SystemRoot* (Stammverzeichnis des Systems) bezeichnet wird und in dem auch Windows installiert wurde. Und selbstverständlich gibt es bei den verschiedenen Windows-Versionen Abweichungen, wo genau dieses Verzeichznis gespeichert ist. Der folgende Abschnitt benennt die Speicherorte wichtiger Ordner.

Die meisten Benutzer und Techniker greifen auf Ordner und Dateien mit einem Werkzeug zu, das in Windows 7 *Windows-Explorer* und in Windows 8/8.1/10 *Datei-Explorer* oder einfach nur *Explorer* heißt. Sie können sich die unterschiedlichen Namen anzeigen lassen, indem Sie mit der rechten Maustaste auf die START-Schaltfläche klicken oder den Mauszeiger über das Ordnersymbol in der Taskleiste platzieren (Abbildung 2.34).

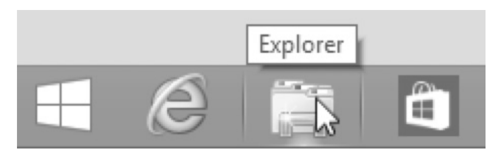


Abb. 2.34: Mauszeiger über dem Ordnersymbol

In Abbildung 2.35 stellt der Explorer den Inhalt des Desktops in Windows 8 dar. Wählen Sie ANSICHT, wenn Sie die Ordneroptionen ändern möchten, um etwa versteckte Dateien und Dateinamenerweiterungen anzuzeigen, allgemeine Optionen zu ändern oder eine andere Ansicht einzustellen.

Im Folgenden wird die zur Beschreibung von Verzeichnisstrukturen vorgesehene Standardformatierung verwendet. Sie wird auch bei der Prüfung 1002 und von fast allen Betriebssystemen verwendet. Windows verbirgt das führende »\«-Zeichen, damit es hübscher aussieht. Wenn der Explorer etwa »Lokale Festplatte (C:) > Benutzer > Mike« anzeigt, wird daraus in der Standardformatierung »C:\Benutzer\Mike«.

C:\Program Files bzw. C:\Programme (Alle Versionen) Standardmäßig installieren die meisten Programme alle oder ihre wichtigsten Dateien in einem Unterverzeichnis des Ordners PROGRAMME. Wenn Sie ein Programm installiert haben, dann sollte es dafür hier einen eigenen Ordner geben. Die jeweiligen Unternehmen bestimmen selbst, wie sie ihre Unterverzeichnisse nennen. Wenn Sie z.B.

Adobe Photoshop installieren, dann wird der Unterordner ADOBE und dann darin das Unterverzeichnis ADOBE PHOTOSHOP erstellt.

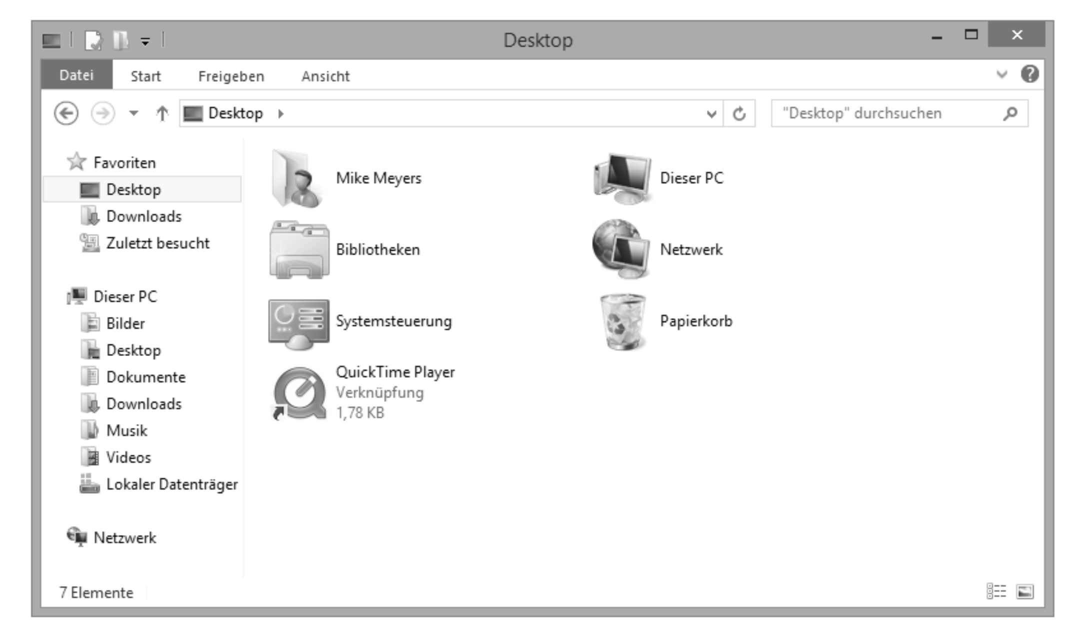


Abb. 2.35: Der Explorer

C:\Program Files (x86) bzw. C:\Programme (x86) Die 64-Bit-Versionen von Windows erstellen zwei Verzeichnisstrukturen für Programmdateien. Die 64-Bit-Anwendungen landen im Ordner `C:\Program Files`, während für die 32-Bit-Anwendungen der Ordner `C:\Program Files (x86)` verwendet wird. Durch diese Trennung lässt sich leicht die richtige Version beliebiger gesuchter Anwendungen ausfindig machen.

Persönliche Dokumente Moderne Windows-Versionen verwenden für die persönlichen Dokumente der verschiedenen Benutzer eines PCs Unterordner des Verzeichnisses `C:\Users` bzw. `C:\Benutzer`. Abbildung 2.36 zeigt die Standardordner eines Benutzers, der Mike heißt. Hier sind diejenigen, die Sie für die CompTIA A+-Prüfung kennen müssen:

- **C:\Benutzer\Mike\Desktop**: In diesem Ordner werden die auf dem Desktop des Benutzers befindlichen Dateien gespeichert. Wenn Sie diesen Ordner löschen, entfernen Sie damit sämtliche auf dem Desktop abgelegten Dateien.
- **C:\Benutzer\Mike\Dokumente**: Hierbei handelt es sich um den Ordner DOKUMENTE bzw. (nur Windows 7) MEINE DOKUMENTE des jeweiligen Benutzers.
- **C:\Benutzer\Mike\Downloads**: Dies ist der von Microsoft vorgegebene Ordner, den Anwendungen bevorzugt für Downloads verwenden sollten. Die meisten Anwendungen verwenden diesen Ordner, manche aber auch nicht.
- **C:\Benutzer\Mike\Musik**: Dieser Ordner ist der Standardspeicherort für heruntergeladene Musik. Ich vermute allerdings, dass die meisten Benutzer ihre Musik eher in iTunes speichern.
- **C:\Benutzer\Mike\Bilder**: Der Ordner BILDER ist der Standardspeicherort für mit dem PC importierte Bilddateien. Die Bibliothek BILDER kann allerdings auf viele weitere Speicherorte zugreifen und macht davon auch regen Gebrauch.
- **C:\Benutzer\Mike\Videos**: VIDEOS ist der Standardspeicherort für Filme und mit dem PC importierte eigene Videoaufnahmen.

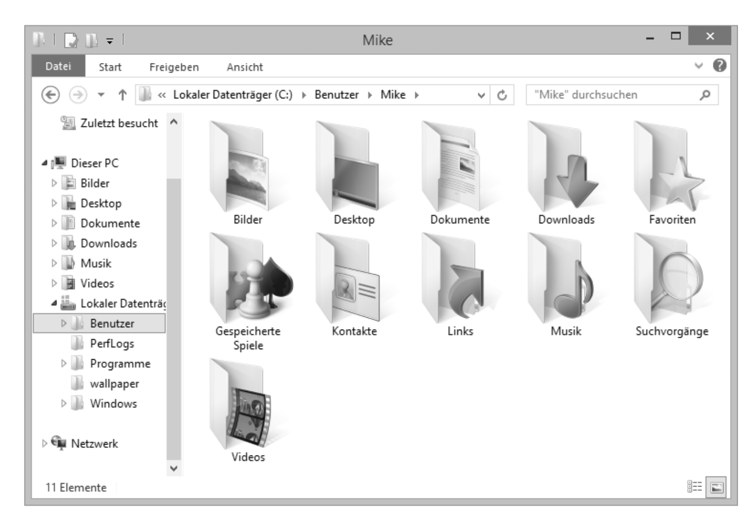


Abb. 2.36: Ordner im Explorer

macOS

In macOS wird der Finder benutzt, um auf Dateien und Ordner zuzugreifen. Abbildung 2.37 zeigt ein Finder-Fenster, das den Inhalt von Mikes Benutzerordner darstellt. Das Design unterscheidet sich zwar von Windows, die Ordner dienen aber denselben Zwecken. Hierbei handelt es sich um die Standardspeicherorte für Dateien auf dem Schreibtisch, für Dokumente, Downloads, Musik, Bilder usw. Jedes Benutzerkonto auf dem Mac verfügt über einen eigenen Benutzerordner, der für die anderen Benutzer des Computers unzugänglich ist.

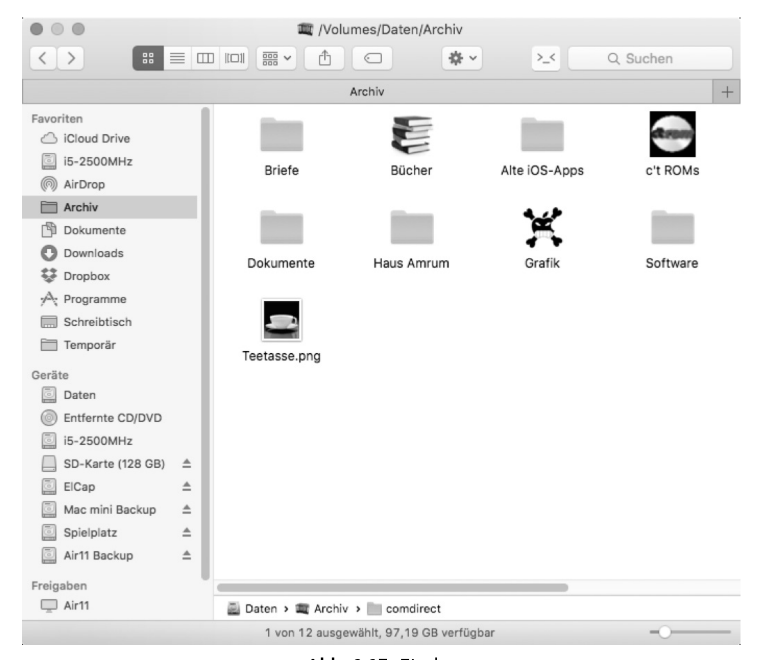


Abb. 2.37: Finder

Linux

Machen Sie sich auf einen Schreck gefasst! Es ist nicht besonders überraschend, dass Linux im Wesentlichen dieselbe Struktur zur Organisation der Benutzer verwendet (Abbildung 2.38). Wenn irgendetwas hinreichend vielen Leuten logisch erscheint, gibt es offenbar keinen Grund, durch Änderungen an dieser Struktur Verwirrung zu stiften. Der einzige bedeutsame Unterschied ist die Bezeichnung: Unter Linux heißt der Ordner nicht USERS bzw. BENUTZER, sondern HOME.



Abb. 2.38: Der HOME-Ordner

2.3.4 Dienstprogramme für Techniker

In jedem Betriebssystem gibt es zwei oder drei Bereiche, in denen Dienstprogramme für Techniker zur Verfügung stehen. In diesem Abschnitt erfahren Sie, wie Sie darauf zugreifen können, damit ich die Schritte nicht ständig wiederholen muss, wenn wir im weiteren Verlauf des Buches immer wieder darauf zugreifen. Wenn Sie sich nicht genau erinnern können, wie man zu einem der Bereiche gelangt, können Sie das einfach in diesem Abschnitt nachschlagen. Außerdem prüft die CompTIA, ob Sie wissen, wie man durch bestimmte Schritte auf die verschiedenen Dienstprogramme zugreift. Nutzen Sie diesen Abschnitt, um Ihr Wissen kurz vor der Prüfung aufzufrischen.

Wichtig

In der CompTIA A+-Prüfung 1002 werden die Pfade zu bestimmten Tools abgefragt. Ihnen werden mehrere solcher Fragen gestellt, und zwar in Form des Multiple-Choice-Verfahrens oder anhand einer vorgegebenen Situation. Es können auch beide Arten von Fragen vorkommen.

Windows 7

In Windows 7 gibt es drei Orte, an denen Sie Dienstprogramme finden: Systemsteuerung, Systemprogramme und Eingabeaufforderung. Sie können auf verschiedene Weise zu diesen Startpunkten für die Dienstprogramme gelangen.

Systemsteuerung Die *Systemsteuerung* ist für die meisten Funktionen zuständig, die mit der Wartung, Aktualisierung und Konfiguration von Windows-Systemen zu tun haben. Sie zählt daher zu den wichtigsten Werkzeugen eines PC-Technikers. Sie können die Systemsteuerung öffnen, indem Sie im Startmenü den Eintrag SYSTEMSTEUERUNG auswählen.

Die Systemsteuerung wird standardmäßig in der Kategorieansicht geöffnet, wobei alle Symbole unter allgemeinen Kategorien zusammengefasst sind, wie beispielsweise Hardware und Sound (Abbildung 2.39). In dieser Ansicht ist ein weiterer Klick erforderlich (und manchmal muss man erraten, welche Kategorie das gesuchte Applet enthält), daher verwenden viele Techniker die klassische Ansicht.

Hinweis

Die Systemsteuerung ermöglicht es, auf den *Geräte-Manager* zuzugreifen, der für Techniker und für die Fehlersuche ein unverzichtbares Werkzeug ist. Mit dem Geräte-Manager können Sie die gesamte Hardware und alle Treiber eines Windows-Computers untersuchen. Nach dieser Beschreibung werden Sie wohl schon vermuten, dass alle Techniker dieses Werkzeug häufig nutzen. Sie werden den Geräte-Manager im weiteren Verlauf dieses Buchs und in Ihrem Berufsleben noch viele Male verwenden.



Abb. 2.39: Systemsteuerung in Windows 7 (Kategorieansicht)

Die CompTIA A+-Prüfung 1002 geht davon aus, dass Sie die klassische Ansicht mit großen Symbolen verwenden. Wechseln Sie also, wie alle Techniker, zur klassischen Ansicht. In Windows 7 können Sie aus der Liste der Ansichten GROSSE SYMBOLE oder KLEINE SYMBOLE auswählen, um einen ähnlichen

Effekt zu erzielen. Abbildung 2.40 zeigt die Systemsteuerung von Windows 7 in der klassischen Ansicht.



Abb. 2.40: Systemsteuerung in Windows 7 (Symbole)

In der Systemsteuerung finden Sie eine Vielzahl von Programmen, die *Applets* genannt werden. Namen und Anzahl der Applets sind bei den verschiedenen Windows-Versionen unterschiedlich und hängen auch davon ab, ob bei Programm- oder Treiberinstallationen weitere Applets hinzugefügt wurden. Viele der Applets gibt es aber in allen Windows-Versionen, wie z.B. ANZEIGE/ANPASSUNG, SOFTWARE/PROGRAMME UND FUNKTIONEN und SYSTEM. Mehr zu den einzelnen Applets erfahren Sie, wenn wir sie im weiteren Verlauf des Buches zum Einsatz bringen.

Systemprogramme Im Menü START finden Sie an zentraler Stelle eine Sammlung technisch orientierter Programme. Im Menü Systemprogramme finden Sie häufig verwendete Dienstprogramme, wie z.B. SYSTEMINFORMATIONEN und DEFRAGMENTIERUNG (Abbildung 2.41).

Viele Techniker denken nicht daran, sich zu merken, wo sie die für die Diagnose von Problemen erforderlichen Programme finden können. Nichts macht sich schlechter, als wenn Sie beim Kunden vor sich hinmurmelnd (»Ich weiß doch, dass das hier irgendwo war.«) in der Gegend herumklicken. In der CompTIA A+-Prüfung 1002 wird daher getestet, ob Sie wissen, auf welchem Weg Sie die entsprechenden Dienstprogramme starten können.

Einer dieser Wege führt in Windows 7 über START|(ALLE) PROGRAMME|ZUBEHÖR|SYSTEMPROGRAMME. Alle Windows-Versionen enthalten einige dieser Werkzeuge, jedoch bringen verschiedene Versionen auch unterschiedliche Dienstprogramme mit. Anstatt die beschriebenen Werkzeuge hier

der Reihe nach vorzustellen, werde ich sie daher an der entsprechenden Stelle im Buch ausführlicher erläutern. Hier ist ein Beispiel, das ansonsten nicht wieder erwähnt wird: die Zeichentabelle.

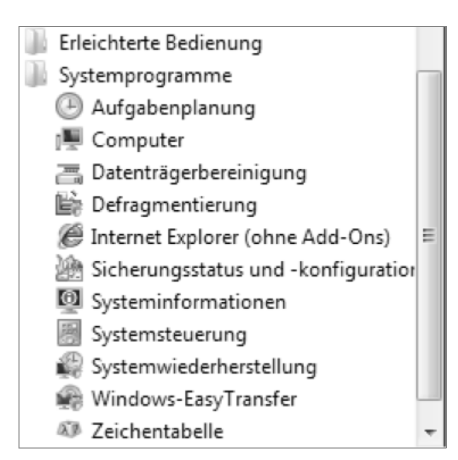


Abb. 2.41: Das Menü SYSTEMPROGRAMME

Haben Sie schon einmal mit einem Programm gearbeitet, in dem Sie ein von der Textverarbeitung nicht unterstütztes Sonderzeichen, wie z.B. das Eurozeichen (€), eingeben wollten? In so einem Fall brauchen Sie die Zeichentabelle (Abbildung 2.42). Mit ihr können Sie beliebige Unicode-Zeichen in die Zwischenablage kopieren und in Ihrem Dokument einsetzen. In Unicode gibt es all die Sonderzeichen und diakritischen Zeichen, die in den Sprachen auf der ganzen Welt zum Einsatz kommen.



Abb. 2.42: Zeichentabelle

Eingabeaufforderung Die Windows-Eingabeaufforderung ist eine Reminiszenz an die Arbeitsweise von Microsoft-Betriebssystemen vor langer, langer Zeit, als noch Textbefehle an einer Eingabeaufforderung eingegeben wurden. Abbildung 2.43 zeigt die Eingabeaufforderung aus DOS, dem ersten auf PCs verbreitet verwendeten Betriebssystem.

```
C:\>ver

MS-DOS Version 6.22

C:\>_
```

Abb. 2.43: DOS-Eingabeaufforderung

DOS ist tot, aber die Eingabeaufforderung gibt es weiterhin unter allen Windows-Versionen. Jeder gute Techniker weiß, wie mit der Eingabeaufforderung umzugehen ist. Sie ist eine große Hilfe, wenn die grafische Benutzeroberfläche von Windows nicht funktioniert, und wenn man sie wirklich beherrscht, dann lässt sich mit ihr häufig schneller als mit der Maus arbeiten. Der Eingabeaufforderung ist ein eigenes Kapitel gewidmet (Kapitel 15). Hier sollen Sie zunächst nur anhand eines Beispiels erfahren, was Sie mit der Eingabeaufforderung anstellen und wie Sie darauf zugreifen können. Klicken Sie auf die START-Schaltfläche, geben Sie in das Feld SUCHE STARTEN `cmd` ein und drücken Sie die Eingabetaste. Abbildung 2.44 zeigt eine Eingabeaufforderung unter Windows 7.

```
Administrator: C:\Windows\System32\cmd.exe
16.01.2010  01:13              478 nssdbm3.chk
16.01.2010  01:13           98.304 nssdbm3.dll
16.01.2010  04:11           87.512 nssutil3.dll
16.01.2010  01:13              139 platform.ini
16.01.2010  04:11           20.440 plc4.dll
16.01.2010  04:11           17.368 plds4.dll
16.02.2010  15:45    <DIR>          plugins
16.01.2010  02:15              229 README.txt
03.02.2010  16:41    <DIR>          res
03.02.2010  16:41    <DIR>          searchplugins
16.01.2010  04:11          103.896 smime3.dll
16.01.2010  01:13              478 softokn3.chk
16.01.2010  01:13          155.648 softokn3.dll
16.01.2010  04:11          458.200 sqlite3.dll
16.01.2010  04:11          136.664 ssl3.dll
03.02.2010  16:41    <DIR>          uninstall
16.01.2010  02:15                3 update.locale
16.01.2010  04:11          243.160 updater.exe
16.01.2010  02:15              701 updater.ini
16.01.2010  04:11           17.880 xpcom.dll
16.01.2010  04:11       11.623.896 xul.dll
              34 Datei(en),     17.236.230 Bytes
              12 Verzeichnis(se), 44.604.833.792 Bytes frei

C:\Program Files (x86)\Mozilla Firefox>
```

Abb. 2.44: Eingabeaufforderung unter Windows 7

Und da Sie sich nun schon einmal an der Eingabeaufforderung befinden, geben Sie doch einfach einmal `dir` ein und betätigen Sie die Eingabetaste. Dieser Befehl zeigt alle Dateien und Ordner in einem bestimmten Verzeichnis (hier wahrscheinlich in Ihrem Benutzerordner) zusammen mit der Dateigröße, Datum und weiteren Angaben an. (Ein Directory ist nichts anderes als ein Ordner.) `dir` ist nur eines der vielen nützlichen Befehlszeilenwerkzeuge, die Sie in diesem Buch kennenlernen werden.

Windows 8/8.1

In Windows 8/8.1 gibt es ebenfalls drei Orte, an denen Sie Dienstprogramme finden, die sich allerdings ein wenig von denjenigen in Windows 7 unterscheiden. Die neueren Versionen umfassen Systemsteuerung, Verwaltung und Eingabeaufforderung.

Systemsteuerung Die Systemsteuerung in Windows 8/8.1 dient demselben Zweck wie in vorhergehenden Windows-Versionen und ist die übliche Anlaufstelle für Dienstprogramme. Sie können auf verschiedene Weise darauf zugreifen:

- Tippen Sie auf den nach unten weisenden Pfeil unten rechts auf dem Startbildschirm und scrollen Sie in der Liste der Apps ganz nach rechts. Klicken Sie in der Kategorie WINDOWS-SYSTEM auf SYSTEMSTEUERUNG (Abbildung 2.45). Das ist der umständliche Weg, den Sie jedoch für die Prüfung kennen sollten. Sie können auch anfangen, in das Suchfeld der App-Liste `Systemsteuerung` einzutippen. Die erwünschte App ist dann schnell unter den besten Treffern.

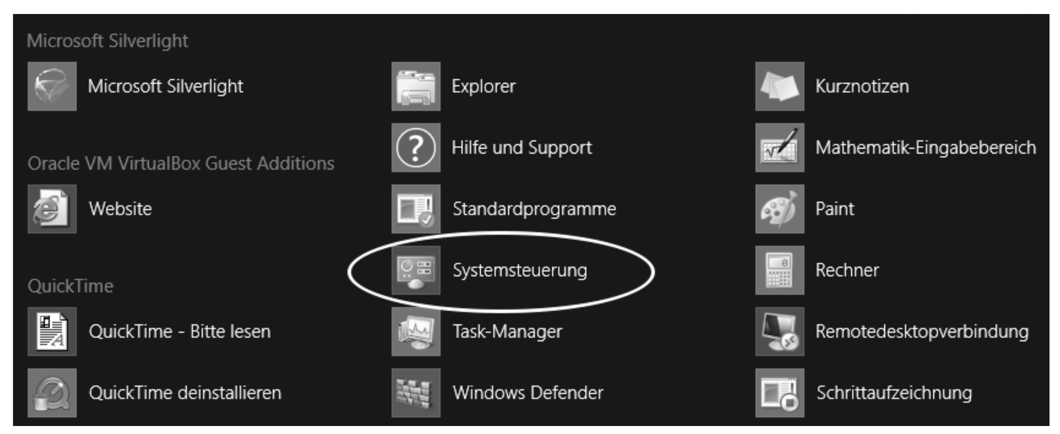


Abb. 2.45: Auswahl der Systemsteuerung in der Liste der Apps

- Klicken Sie mit der rechten Maustaste auf die START-Schaltfläche und wählen Sie den Menüpunkt SYSTEMSTEUERUNG aus (Abbildung 2.46). Sie können sich dasselbe Menü auch durch Drücken der Tastenkombination [Win] + [X] anzeigen lassen.

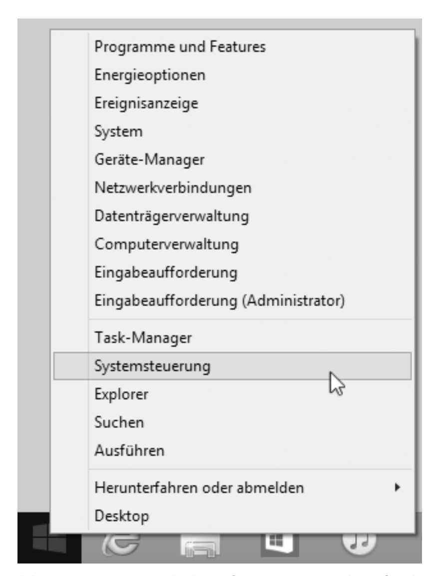


Abb. 2.46: Rechtsklick auf die START-Schaltfläche

Ich bezeichne dieses Menü als »technische Grundlagen«, weil es nicht nur sehr schnell Zugriff auf die Systemsteuerung und die dazugehörige Werkzeugsammlung ermöglicht, sondern auch Zugang zu bestimmten Dienstprogrammen bietet, die für jeden Techniker unverzichtbar sind, wie z.B. der Task-Manager (um unter anderem etwa eingefrorene Programme zu beenden).

- Fangen Sie bei angezeigtem Startbildschirm an, `Systemsteuerung` einzutippen. Im Charm SUCHEN erscheint dann die Systemsteuerung als Top-Treffer (Abbildung 2.47). Wählen Sie ihn aus, um die Systemsteuerung zu öffnen.

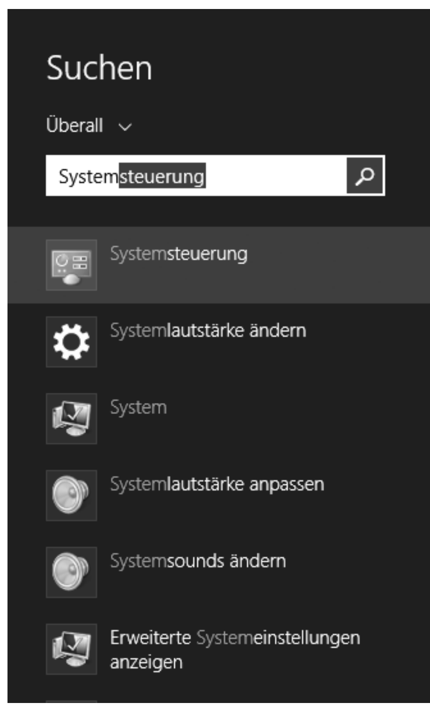


Abb. 2.47: Der Charm SUCHEN mit der Systemsteuerung als Top-Treffer

Verwaltung Seit dem Erscheinen von Windows 8 hat Microsoft das Werkzeug VERWALTUNG immer wieder aufgepeppt und einige der Dienstprogramme integriert, die in älteren Windows-Versionen unter den Systemprogrammen zu finden waren. VERWALTUNG gestattet es, Festplatten einzurichten, Geräte zu handhaben, die Systemleistung zu testen und vieles andere mehr. Diese Werkzeugsammlung ist für jeden Techniker unentbehrlich und wir werden sie bei den Beispielen in diesem Buch immer wieder verwenden.

Wie bei der Systemsteuerung gibt es verschiedene Möglichkeiten, auf VERWALTUNG zuzugreifen:

- Klicken Sie auf dem Startbildschirm auf den nach unten weisenden Pfeil, um die Liste der Apps anzuzeigen. Wenn Sie ein wenig nach rechts scrollen, erscheint eine Liste der Windows-Systemprogramme (Abbildung 2.48). Wählen Sie das Werkzeug aus, das Sie öffnen möchten.
- Fangen Sie bei angezeigtem Startbildschirm an, `Verwaltung` einzutippen. Im Charm SUCHEN erscheint dann VERWALTUNG schon bald als Top-Treffer, den Sie zum Öffnen auswählen können (Abbildung 2.49).
- Klicken Sie mit der rechten Maustaste auf die START-Schaltfläche (oder drücken Sie die Tastenkombination [Win] + [X]) und wählen Sie im Kontextmenü den Punkt SYSTEMSTEUERUNG aus. Wählen Sie dann in der Systemsteuerung VERWALTUNG aus.

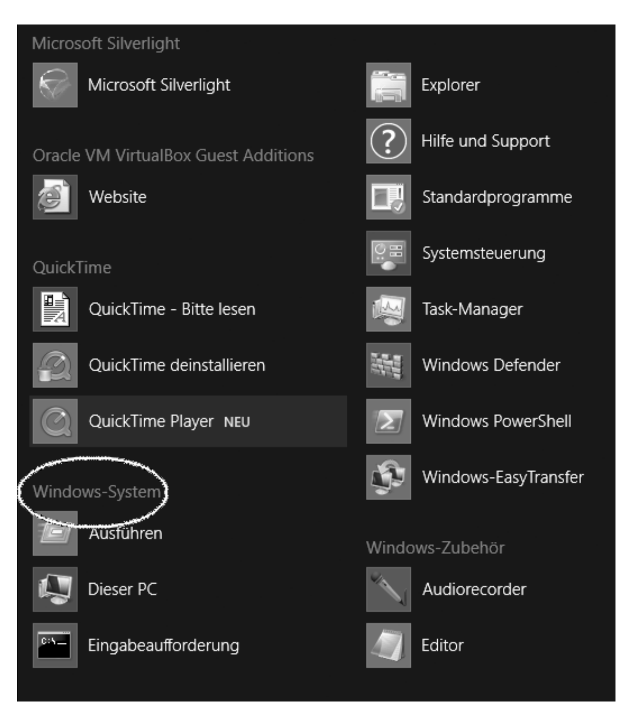


Abb. 2.48: Windows-Systemprogramme in der Liste der Apps

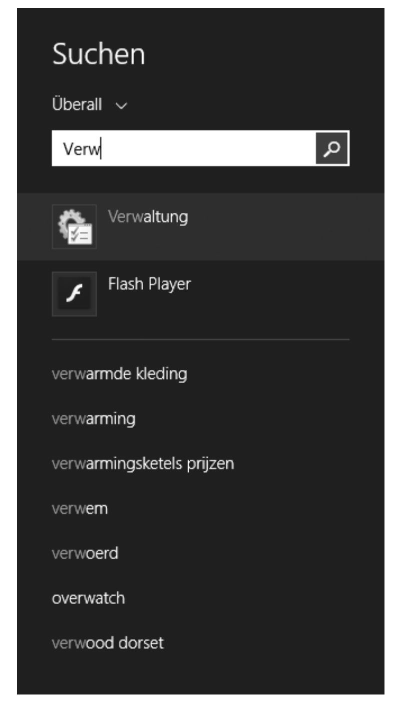


Abb. 2.49: VERWALTUNG als Top-Treffer im Charm SUCHEN

Eingabeaufforderung Die Eingabeaufforderung ist und bleibt für Techniker unverzichtbar. Windows 8/8.1 bietet mehrere Zugriffsmöglichkeiten:

- Tippen oder klicken Sie auf dem Startbildschirm unten rechts auf den nach unten weisenden Pfeil und scrollen Sie in der Liste der Apps nach ganz rechts. Klicken Sie in der Kategorie WINDOWS-SYSTEM auf EINGABEAUFFORDERUNG um das Programm zu öffnen. Sie können auch in das Suchfeld der App-Liste `Eingabeaufforderung` eintippen und das Programm unter den Treffern auswählen.
- Klicken Sie mit der rechten Maustaste auf die START-Schaltfläche (oder drücken Sie die Tastenkombination [Win] + [X]) und wählen Sie im Kontextmenü den Punkt EINGABEAUFFORDERUNG aus.
- Fangen Sie bei angezeigtem Startbildschirm an, `cmd` oder `Eingabeaufforderung` einzutippen. Im Charm SUCHEN erscheint dann die EINGABEAUFFORDERUNG unter den Top-Treffer. Klicken Sie darauf, um sie zu öffnen.

Windows 10

Auch in Windows 10 bleibt die aus älteren Windows-Versionen bekannte Systemsteuerung erhalten und die Eingabeaufforderung gibt es ebenfalls weiterhin. Zusätzlich gibt es jedoch eine erweiterte Einstellungs-App zur alltäglichen Administration. Darüber hinaus ist eine erheblich leistungsfähigere Kommandozeilenschnittstelle namens Windows PowerShell verfügbar, die sehr viel umfassendere Kommandozeilenwerkzeuge bietet und Skripte unterstützt. In Kapitel 15 erfahren Sie mehr über die PowerShell (siehe Abbildung 2.50).

```
Windows PowerShell
PS C:\Windows> cd System32
PS C:\Windows\System32> Get-Eventlog -Log System -Newest 20

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    1421 Sep 22 16:40  Information Service Control M...   1073748864 Der Starttyp des Diensts "Intelligenter Hinterg...
    1420 Sep 22 16:40  Information Microsoft-Windows...           19 Installation erfolgreich: Das folgende Update w...
    1419 Sep 22 16:40  Information Microsoft-Windows...           43 Installation gestartet: Windows hat mit der Ins...
    1418 Sep 22 16:40  Information Microsoft-Windows...           44 Windows Update hat mit dem Herunterladen eines ...
    1417 Sep 22 16:38  Information Service Control M...   1073748864 Der Starttyp des Diensts "Intelligenter Hinterg...
    1416 Sep 22 16:37  Information Microsoft-Windows...         7001 Benutzeranmeldebenachrichtigung für Programm zu...
    1415 Sep 22 16:34  Information Microsoft-Windows...            1 Das System wurde aus einem Standbymodus reaktiv...
    1414 Sep 22 16:34  Information Microsoft-Windows...           27 Die Beschreibung für Ereignis-ID 27 in Quelle M...
    1413 Sep 22 16:34  Information Microsoft-Windows...           25 Die Beschreibung für Ereignis-ID 25 in Quelle M...
    1412 Sep 22 16:34  Information Microsoft-Windows...           32 Die Beschreibung für Ereignis-ID 32 in Quelle M...
    1411 Sep 22 16:34  Information Microsoft-Windows...           18 Die Beschreibung für Ereignis-ID 18 in Quelle M...
    1410 Sep 22 16:34  Information Microsoft-Windows...           30 Die Beschreibung für Ereignis-ID 30 in Quelle M...
    1409 Sep 22 16:34  Information TXEIx64                1074200578 Intel(R) Trusted Execution Engine Interface dri...
    1408 Sep 22 16:34  Information EventLog               2147489661 Die aktive Systemzeit ist 243199 Sekunden.
    1407 Sep 22 16:34  Information Microsoft-Windows...            1 Mögliche CVE-Erkennung: 2019-09-22T14:34:26.500...
    1406 Sep 20 22:27  Information Microsoft-Windows...          107 Die Beschreibung für Ereignis-ID 107 in Quelle ...
    1405 Sep 20 22:27  Information BROWSER                1073749857 Der Suchdienst hat eine Wahl auf dem Netzwerk "...
    1404 Sep 20 22:27  Information Microsoft-Windows...           42 Die Beschreibung für Ereignis-ID 42 in Quelle M...
    1403 Sep 20 22:27  Information Microsoft-Windows...          187 Die Beschreibung für Ereignis-ID 187 in Quelle ...
    1402 Sep 20 22:27  Information Win32k                 1073742091 Die Qualitätssicherungsüberprüfung für Fingerei...

PS C:\Windows\System32> _
```

Abb. 2.50: Die PowerShell in Windows 10

Hinweis

Die Windows PowerShell gibt es schon eine ganze Weile, länger als Windows 7. Allerdings wurde sie sechs Mal stark überarbeitet, sodass sie in Windows 10 erheblich leistungsfähiger ist als die ursprünglichen Versionen. Wenn Sie in Windows 10 mit der rechten Maustaste auf das Startmenü klicken, wird als Kommandozeilenschnittstelle standardmäßig die PowerShell angeboten. Sie können aber weiterhin auf die ältere Kommandozeile (`cmd.exe`) zugreifen, indem Sie im Suchfeld in der Taskleiste `cmd` oder `command` eingeben.

Systemsteuerung Windows 10 bietet zwei Standardmethoden zum Aufruf der Systemsteuerung. Klicken Sie mit der rechten Maustaste auf die START-Schaltfläche, um das Menü mit den technischen Grundlagen zu öffnen und wählen Sie SYSTEMSTEUERUNG aus. Alternativ können Sie auf die Start-Schaltfläche klicken, um die Metro/Modern-UI-Oberfläche zu öffnen, `Systemsteuerung` eintippen und die App unter den Suchergebnissen auswählen.

Einstellungs-App Die *Einstellungs-App* von Windows 10 kombiniert eine Vielzahl von Dienst- und Hilfsprogrammen sowie weiteren Tools, die eigentlich in keinerlei Verbindung stehen und ansonsten weit über das gesamte System verteilt sind, zu einer einigermaßen einheitlichen Windows-App (Abbildung 2.51). Seit die Einstellungs-App mit Windows 8 eingeführt wurde, hat sie immer mehr Aufgaben der Systemsteuerung übernommen. Es ist damit zu rechnen, dass sie weiter wächst, wenn Windows 10 allmählich heranreift.

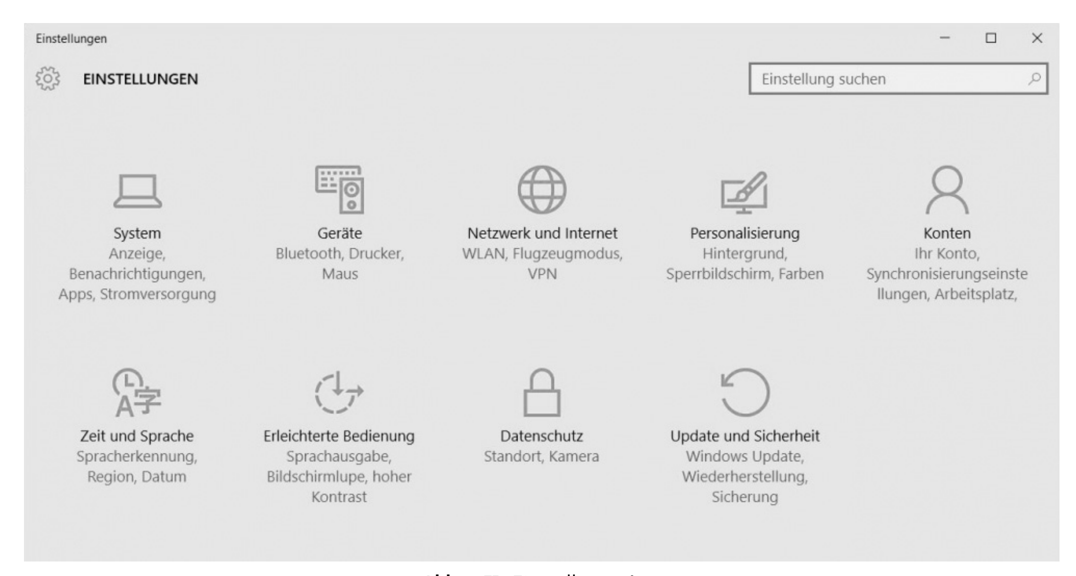


Abb. 2.51: Einstellungs-App

Gehen Sie folgendermaßen vor, um auf die Einstellungs-App zuzugreifen: Drücken Sie zum Öffnen des Startmenüs die Taste [Win] und wählen Sie dann unten links EINSTELLUNGEN aus, um die App zu öffnen (Abbildung 2.52).

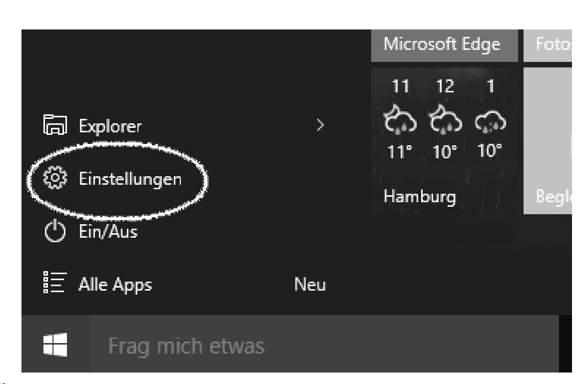


Abb. 2.52: Öffnen der Einstellungen in Windows 10. Beachten Sie, dass die PowerShell die Standardkommandozeile ist.

macOS

In macOS gibt es für Techniker zwei wichtige Bereiche, nämlich das Programm SYSTEMEINSTELLUNGEN und den Ordner DIENSTPROGRAMME. Auf beide können Sie schnell zugreifen.

Systemeinstellungen Klicken Sie auf den in allen Anwendungen sichtbaren Apfel in der linken oberen Ecke des Bildschirms und wählen Sie den Menüpunkt SYSTEMEINSTELLUNGEN ... aus, um das Programm zu öffnen (Abbildung 2.53).



Abb. 2.53: Öffnen der Systemeinstellungen

Ordner Dienstprogramme Der zweite Ort von Interesse ist der Ordner DIENSTPROGRAMME, der sich wiederum im Ordner PROGRAMME befindet. Da er so wichtig ist, stellt Apple eine Abkürzung zur Verfügung, um darauf zuzugreifen. Wählen Sie im Finder im Menü GEHE ZU den Punkt DIENSTPROGRAMME aus, um den Ordner zu öffnen (Abbildung 2.54). Alternativ können Sie auch die Tastenkombination [⇧] + [⌘] + [U] verwenden. Sie erhalten damit Zugriff auf die Dienstprogramme, die Sie für Aufgaben benötigen, die über die in den Systemeinstellungen verfügbaren Möglichkeiten hinausgehen, beispielsweise die AKTIVITÄTSANZEIGE oder das Programm TERMINAL. Letzteres ist die Schnittstelle zur Kommandozeile für macOS, ein äußerst mächtiges Werkzeug für Techniker, auf das ich in Kapitel 15 näher eingehe.



Abb. 2.54: Öffnen des Ordners DIENSTPROGRAMME

Linux

Unter Linux ist die Kommandozeile, die als Terminal bezeichnet wird, für Techniker unentbehrlich. In den meisten Distributionen kann sie durch die Tastenkombination `Strg` + `Alt` + `T` aufgerufen werden. (In Kapitel 15, *Eingabeaufforderung*, finden Sie Details zu den wichtigsten Linux-Befehlen.)

Der Zugriff auf Dienst- und Hilfsprogramme ist von Distro zu Distro unterschiedlich. Nachstehend finden Sie die Methoden der beiden gebräuchlichsten Desktop-Umgebungen.

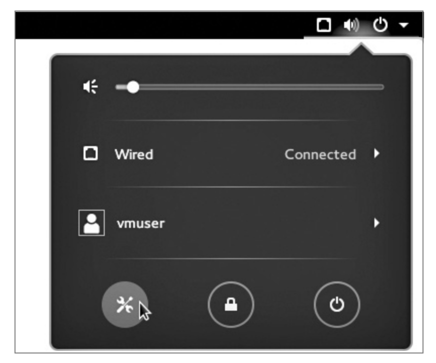


Abb. 2.55: Zugriff auf alle Einstellungen

Einstellungen und Dienstprogramme, die nicht Bestandteil der Systemeinstellungen sind, finden Sie über den Dateibrowser. Klicken Sie auf das Ubuntu-Symbol am oberen Ende der Startleiste. Hier können Sie herumstöbern oder nach praktischen Werkzeugen wie dem Systemmonitor oder dem stets benötigten Terminal suchen (Abbildung 2.56).

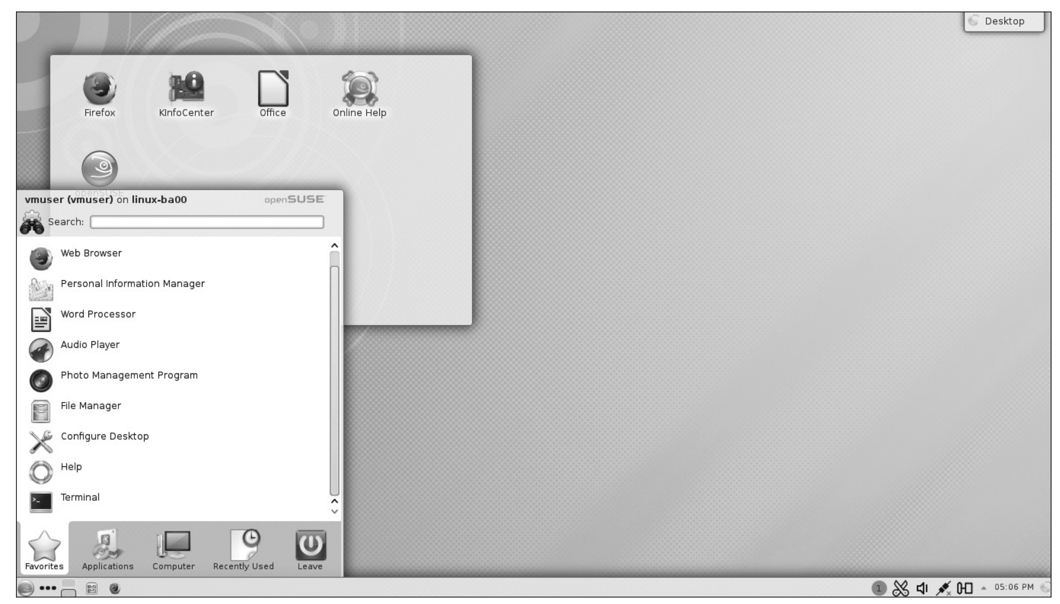


Abb. 2.56: KDE Kickoff-Menü

GNOME 3 Der erste Ausgangspunkt in einer GNOME-3-Desktop-Umgebung ist die Anwendung ALLE EINSTELLUNGEN. Klicken Sie auf den nach unten weisenden Pfeil am rechten Ende der Menü-

leiste und wählen Sie das Schraubendreher-/Schraubenschlüssel-Symbol aus, um darauf zuzugreifen (Abbildung 2.55).

Klicken Sie auf die Schaltfläche AKTIONEN auf der linken Seite der Menüleiste, um andere Dienstprogramme wie SYSTEMMONITOR oder TERMINAL aufzurufen. Hier können Sie mittels des Eingabefelds nach Programmen suchen. Dann wird ein Menü mit allen installierten Programmen angezeigt, das auch einen Ordner mit den Dienstprogrammen enthält.

KDE Plasma Desktop Das inoffizielle Motto für Linux könnte »Auswahl!« lauten, und wenn Sie eine KDE-basierte Distribution verwenden, sind Sie in dieser Hinsicht zweifelsohne verwöhnt. Der Nachteil dieser Vielfalt besteht darin, dass sich die Konfigurationswerkzeuge der verschiedenen KDE-Distros oft deutlich voneinander unterscheiden.

Eines ist jedoch allen auf KDE beruhenden Distros gemeinsam: Alles, was Sie zur Nutzung des Systems benötigen, ist über das Kickoff-Menü am linken Ende der Menüleiste erreichbar (Abbildung 2.56). Das Kickoff-Menü ist dem Startmenü in Windows 7 optisch und funktional sehr ähnlich und sollte daher leicht verständlich sein. Im Kickoff-Menü können Sie nach einem Programm suchen oder sich auf einer Registerkarte die vorhandenen Programme anzeigen lassen. Hier findet sich in den meisten Distributionen ein Menüpunkt, über den man auf die wichtigsten Systemeinstellungen und Dienstprogramme zugreifen kann.

2.4 Wiederholung

2.4.1 Fragen

1. Mit welcher Windows-Version wurde Metro UI eigeführt?
   A. Windows 7
   B. Windows 8
   C. Windows 8.1
   D. Windows 10
2. Welche Funktionalität von Windows 8 hat Microsoft in Windows 10 weggelassen?
   A. Metro/Modern UI
   B. Startmenü
   C. Systemsteuerung
   D. Charm-Leiste
3. Welche Funktionalität von macOS entspricht im Wesentlichen mehreren Desktops?
   A. Charms
   B. Schreibtisch
   C. Mission Control
   D. Spaces
4. Welches KDE-Feature entspricht im Wesentlichen dem Startmenü?
   A. Metro UI
   B. Kickoff
   C. Terminal
   D. GNOME 3
5. Der Benutzer Mike hat mit seinem Webbrowser Dateien heruntergeladen. Wo werden diese standardmäßig gespeichert?
   A. `C:\Downloads`
   B. `C:\Mike\Desktop\Downloads`
   C. `C:\Users\Mike\Downloads`
   D. `C:\Users\Mike\Desktop\Downloads`

6. In welchem Ordner werden auf einer 64-Bit-Version von Windows standardmäßig 32-Bit-Programme installiert?
   A. C:\Program Files
   B. C:\Program Files (x32)
   C. C:\Program Files\Wins\Old
   D. C:\Program Files (x86)
7. Welche Funktionalität von macOS entspricht dem Windows-Explorer?
   A. Finder
   B. Dock
   C. Quartz
   D. Dateiverwaltung
8. Wie kann man unter Windows 8.1 die App COMPUTERVERWALTUNG öffnen?
   A. Rechtsklick auf die Taskleiste und Auswahl von COMPUTERVERWALTUNG im Kontextmenü.
   B. Rechtsklick auf die START-Schaltfläche und Auswahl von COMPUTERVERWALTUNG im Kontextmenü.
   C. Rechtsklick irgendwo auf dem Desktop und Auswahl von COMPUTERVERWALTUNG im Kontextmenü.
   D. Mit der Tastenkombination ⊞ + L
9. Welche Funktionalität von macOS entspricht der Eingabeaufforderung?
   A. Dock
   B. Spaces
   C. Terminal
   D. Unity
10. Welche App von Windows 10 vereinigt verschiedene Hilfsprogramme in einem einzigen Dienstprogramm?
   A. Einstellungs-App
   B. Steuerung
   C. Befehlscenter
   D. Systemcenter

2.4.2 Antworten

1. **B.** Microsoft hat Metro UI mit Windows 8 eingeführt.
2. **D.** Microsoft hat in Windows 10 die Charm-Leiste weggelassen. Auf Wiedersehen!
3. **D.** Für mehrere Desktops verwendet Apple in macOS den Ausdruck *Spaces*.
4. **B.** Das Kickoff-Menü funktioniert wie das Startmenü.
5. **C.** Der Standardspeicherort für heruntergeladene Dateien in Windows ist C:\Users\<Benutzername>\Downloads.
6. **D.** Standardmäßig werden 32-Bit-Programme im Ordner C:\Program Files (x86) installiert.
7. **A.** Das Pendant zum Windows-Explorer ist der Finder.
8. **B.** Klicken Sie mit der rechten Maustaste auf die START-Schaltfläche und wählen Sie im Kontextmenü COMPUTERVERWALTUNG. Ein Kinderspiel!
9. **C.** Das Pendant zur Eingabeaufforderung ist das Dienstprogramm TERMINAL.
10. **A.** In Windows 10 bietet die Einstellungs-App eine Vielzahl von Hilfsprogrammen unter einer einheitlichen Oberfläche an.

Mikroprozessoren 3

Themen in diesem Kapitel:

- Komponenten eines Prozessors
- CPUs und der Zugriff auf den Arbeitsspeicher (RAM)
- Die Vielfalt aktueller CPUs
- Auswahl der passenden CPU und deren Einbau
- Fehlerbehebung

Die CPU erledigt die meisten der Berechnungen, die Ihren Computer erst zu einem, nun ja, *Computer* machen. Die *CPU* (*Central Processing Unit*), die auch als *Mikroprozessor* oder kurz *Prozessor* bezeichnet wird, versteckt sich auf dem Mainboard hinter großen Kühlrippen und oft auch hinter einem Lüfter. Die Produzenten von CPUs gehen ähnlich wie die Hersteller in der Autoindustrie vor und geben ihren Prozessoren Namen und Modellbezeichnungen wie etwa Intel Core i9, Qualcomm Snapdragon 835 oder AMD Ryzen 7. Aber was passiert innerhalb einer CPU, damit sie all die erstaunlichen Dinge erledigen kann, die Sie ständig von ihr verlangen?

Ich werde mich in diesem Kapitel intensiv mit Mikroprozessoren beschäftigen. Zunächst erläutere ich die Funktionsweise des Prozessors und der Komponenten, die es ihm ermöglichen, mit anderen Teilen des Computers zusammenzuarbeiten. Im zweiten Abschnitt wird beschrieben, wie der Prozessor auf den Arbeitsspeicher zugreift. Der dritte Abschnitt stellt Ihnen moderne CPUs vor. Im vierten Abschnitt geht es um die Praxis, nämlich die Auswahl und Installation von CPUs. Im letzten Abschnitt schließlich betrachte ich ausführlich die Fehlerbehebung.

Wichtig

In den CompTIA-Prüfungen wird normalerweise der Begriff *CPU* verwendet, nicht Mikroprozessor.

Geschichte und Konzepte

3.1 Kernkomponenten der CPU

Computer scheinen zwar einigermaßen intelligent zu sein, jedoch würde jeder Vergleich einer CPU mit dem menschlichen Gehirn eine ziemliche Übertreibung ihrer Fähigkeiten darstellen. Eine CPU arbeitet weniger wie ein Gehirn, sondern mehr wie eine sehr leistungsfähige Rechenmaschine – und was für eine! Die heutigen CPUs können Milliarden von Zahlen je Sekunde addieren, subtrahieren, multiplizieren, dividieren und im Speicher verschieben. Durch diese beträchtliche Leistungsfähigkeit wirken Mikroprozessoren recht intelligent. Tatsächlich handelt es sich aber um keine echte Intelligenz, sondern um pure Geschwindigkeit, durch die moderne CPUs so intelligent zu sein scheinen und durch die sie Aufgaben bewältigen können, wie z.B. den Zugriff aufs Internet, die Darstellung optisch atemberaubender Spiele oder die Bearbeitung digitaler Bilder.

Gute PC-Techniker müssen, um Servicearbeiten am PC durchführen zu können, die grundlegenden Funktionen einer CPU kennen. Als Erstes werden Sie daher erfahren, wie die CPU arbeitet. Dazu verwende ich ein ganz einfaches Beispiel, denn wenn Sie jemandem erklären wollen, wie ein Automotor funktioniert, würden Sie dafür doch auch ein relativ einfaches Beispiel wählen, oder? Dasselbe gilt auch für CPUs. Die für die folgenden Beispiele verwendete CPU ist der berühmte Intel 8088, der in den späten 1970er-Jahren entwickelte Urahn aller modernen Mikroprozessoren. Obwohl es ihn

bereits vor mehr als 40 Jahren gab, enthalten selbst die modernsten CPUs immer noch dieselben Grundbausteine wie ihr Urahn.

3.1.1 Der Mann in der Schachtel

Stellen Sie sich die CPU zunächst als einen recht gewitzten Mann in einer Schachtel vor (Abbildung 3.1). Dieser Mann ist ein Rechengenie und beherrscht praktisch alle mathematischen Funktionen und Datenmanipulationen und kann alle Fragen *äußerst schnell* beantworten.

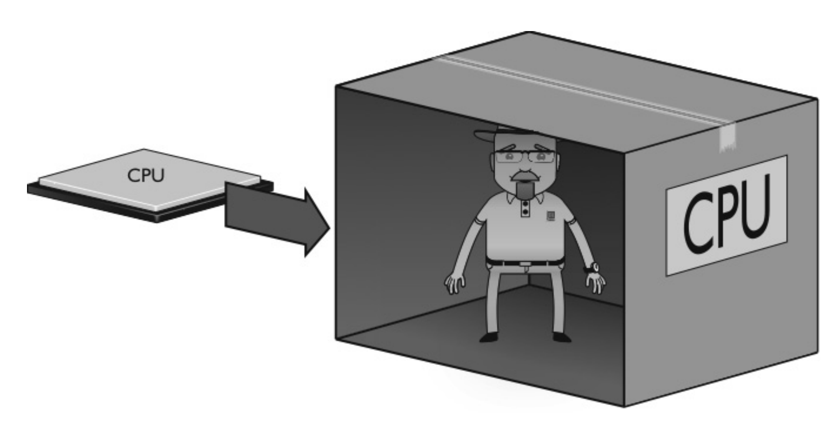


Abb. 3.1: Stellen Sie sich die CPU wie einen Mann in einer Schachtel vor!

Sie möchten nun gern, dass Ihnen dieser Mann bei der Arbeit hilft, haben aber ein Problem, denn er kann nichts wahrnehmen, was außerhalb der Schachtel geschieht. Bevor er mit uns zusammenarbeiten kann, müssen wir daher eine Möglichkeit finden, um Informationen mit ihm auszutauschen (Abbildung 3.2).

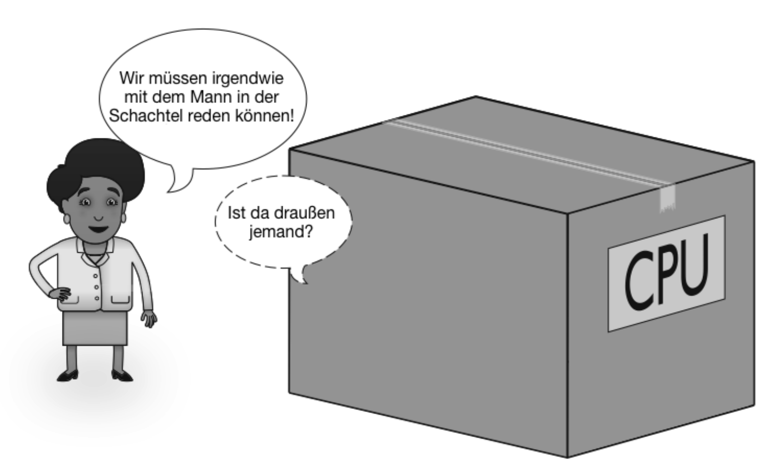


Abb. 3.2: Wie können wir mit dem Mann in der Schachtel kommunizieren?

Stellen Sie sich vor, wir würden 16 Glühbirnen installieren, von denen sich acht innerhalb und acht außerhalb der Schachtel befinden. Jede Glühbirne im Innern der Schachtel ist paarweise mit einer anderen außerhalb der Schachtel verbunden. Jedes Birnenpaar ist entweder ein- oder ausgeschaltet. Wir können die acht Birnenpaare über eine Reihe von acht Schaltern außerhalb der Schachtel steuern

und auch der Mann in der Schachtel kann sie über acht identische Schalter steuern. Diese Glühbirnenkommunikation nennen wir den *externen Datenbus (EDB)*.

Abbildung 3.3 zeigt das Modell eines externen Datenbusses. Wenn wir oder der Mann in der Schachtel einen Schalter betätigen, leuchten *beide* Glühbirnen, und auch der Schalter auf der anderen Seite wird gleichzeitig wie von Zauberhand bewegt. Bringen wir oder der Mann in der Schachtel einen Schalter in die Aus-Position, gehen die Birnen auf beiden Seiten aus und auch der andere Schalter wechselt entsprechend seine Position.

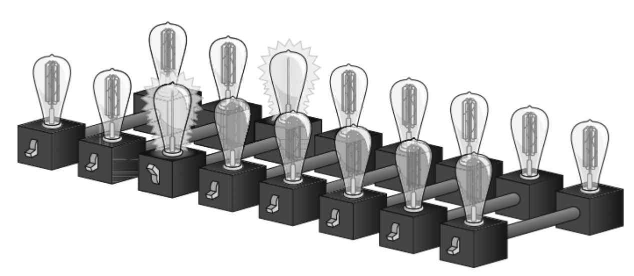


Abb. 3.3: Einblick in den externen Datenbus. Beachten Sie, dass ein Glühbirnenpaar eingeschaltet ist.

Erkennen Sie, wie diese Anordnung funktioniert? Über verschiedene Lichtmuster können wir nun wechselseitig mit dem Mann in der Schachtel kommunizieren und Informationen austauschen. Damit das funktioniert, müssen aber beide Seiten *vorher vereinbart haben, was die verschiedenen Lichtmuster bedeuten sollen.* Dazu wird eine Art Codebuch benötigt, in dem die Bedeutung der verschiedenen Lichtmuster verzeichnet ist. Denken Sie immer daran, während ich unsere Analogie noch ein wenig fortsetze.

Bevor wir uns weiteren Details zuwenden, sollten Sie sich darüber klar sein, dass es sich hier nur um eine Analogie und nicht um die Realität handelt. Es gibt zwar wirklich einen EDB, jedoch keinen mit Glühbirnen oder Schaltern. Allerdings können Sie die feinen Leitungen sehen, die zur CPU führen (Abbildung 3.4.Wenn Sie an diesen Leitungen Spannungen anlegen, machen Sie im Grunde genommen nichts anderes, als einen Schalter umzulegen. Verstehen Sie das Prinzip? Wenn eine dieser Leitungen nun unter Spannung steht und eine winzige Glühbirne angeschlossen wäre, dann würde diese leuchten. Und natürlich würde die angeschlossene Birne nicht leuchten, wenn die Leitung keine Spannung führt. Aus diesem Grund verwenden wir hier die Analogie mit Glühbirnen und Schaltern. Mit ihrer Hilfe können Sie sich diese feinen Leitungen mit ihren kontinuierlich wechselnden Spannungszuständen besser vorstellen.

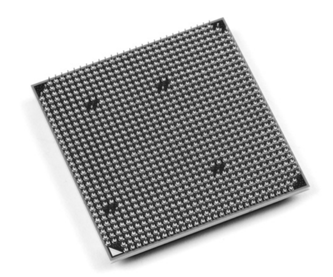


Abb. 3.4: Ansicht der Unterseite einer CPU

Nun können wir über den externen Datenbus mit dem Mann in der Schachtel kommunizieren und uns ansehen, was passiert, wenn wir Spannung an die Leitungen anlegen. Damit entsteht aber ein gewisses Begriffsproblem. Wenn man über Leitungen spricht, an denen Spannung anliegt oder nicht, wäre es recht mühsam, »Ein-Aus-Aus-Aus-Ein-Ein-Aus-Aus« zu sagen. Daher sagt man nicht, dass eine der Leitungen des externen Datenbusses ein- oder ausgeschaltet ist. Vielmehr verwendet man die Zahl

1, wenn Spannung anliegt (Zustand eingeschaltet), und die Zahl 0, wenn an einer Leitung keine Spannung anliegt (Zustand ausgeschaltet; Abbildung 3.5). So lässt sich der Zustand der Birnen statt mit »Ein-Aus-Aus-Aus-Ein-Ein-Aus-Aus« auch mit »10001100« beschreiben.



Abb. 3.5: »1« bedeutet eingeschaltet und »0« bedeutet ausgeschaltet.

Bei Computern werden Leitungen ständig ein- und wieder ausgeschaltet. Aus diesem Grund wird das System mit den Einsen und Nullen, das auch *binäres* oder *duales Zahlensystem* genannt wird, zur Darstellung der verschiedenen Zustände verwendet. (Haben Sie etwa geglaubt, dass Computernarren Binärzahlen nur deshalb verwenden, um die übrige Menschheit zu verwirren? Ha!) Eigentlich gäbe es noch weit mehr über das binäre Zahlensystem zu sagen. Für den Anfang mag dies aber genügen.

3.1.2 Register

Der Mann in der Schachtel ist gut geeignet, um die Funktionsweise einer CPU zu verdeutlichen. Über den externen Datenbus können wir wechselseitig mit dem Mann in der Schachtel kommunizieren und ihm auch Aufgaben stellen. Dazu benötigt er aber einen Arbeitstisch. Tatsächlich benötigt er sogar mindestens vier Arbeitstische. Auf jedem dieser vier Tische befinden sich 16 Glühbirnen. Diese Birnen sind nicht paarweise miteinander verbunden. Es sind einfach 16 auf dem Tisch aufgereihte Glühbirnen, die jeweils über einen einzelnen Schalter gesteuert und nur von dem Mann in der Schachtel bedient werden können. Durch Erzeugen von Ein/Aus-Mustern wie auf dem externen Datenbus kann der Mann in der Schachtel mathematische Aufgabenstellungen mithilfe der vier Birnenreihen lösen. Bei Computern nennt man diese Arbeitstische Register (Abbildung 3.6). Mit ihrer Hilfe werden interne Befehle und Daten gespeichert.

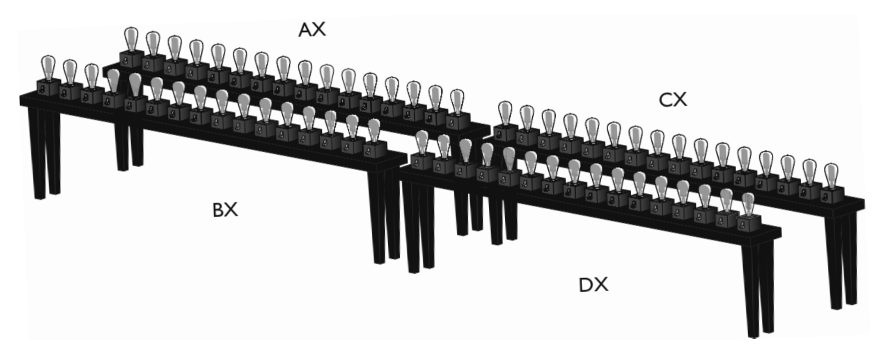


Abb. 3.6: Die vier allgemeinen Register

Mit den Registern kann der Mann in der Schachtel ihm gestellte Aufgaben bearbeiten. Alle CPUs enthalten zwar eine Vielzahl von Registern, hier werde ich mich aber auf jene vier Register beschränken, die am häufigsten benutzt und Mehrzweckregister genannt werden. Intel hat ihnen die Namen AX, BX, CX und DX gegeben.

Hinweis

Der Intel 8088 war der erste Prozessor, der die mittlerweile berühmten vier Mehrzweckregister AX-DX verwendete, die es auch in den neuesten Prozessoren noch gibt. (Allerdings mit sehr viel mehr Glühbirnen!) Bei 32-Bit-Prozessoren wird ein »E« (für *extended*, also erweitert) vorangestellt und die Register heißen EAX, EBX usw. Bei 64-Bit-Prozessoren wird ein »R« verwendet (dessen Bedeutung mir nicht bekannt ist) und die Register heißen RAX, RBX usw.

So weit, so gut! Nun kann der Mann in der Schachtel schon fast seine Arbeit aufnehmen. Bevor wir aber den Deckel der Schachtel wieder schließen, müssen wir dem Schachtelmann noch ein weiteres Werkzeug mitgeben. Erinnern Sie sich noch an das erwähnte Codebuch? Wir werden jetzt eines erstellen, mit dessen Hilfe wir uns mit ihm verständigen können. Abbildung 3.7 zeigt das Codebuch, das wir verwenden werden und von dem es Kopien für uns und den Schachtelmann gibt.

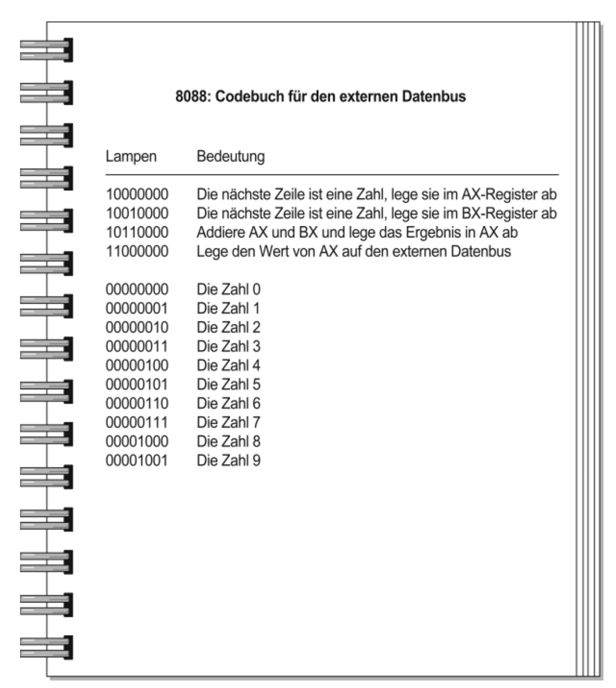


Abb. 3.7: Das CPU-Codebuch

In diesem Codebuch bedeutet 10000111 z.B. *»Verschiebe die Zahl 7 in das Register AX«*. Bei derartigen Befehlen handelt es sich um die *Maschinensprache* des Mikroprozessors. Bei den im obigen Codebuch aufgeführten Befehlen handelt es sich um keine echten Maschinenbefehle. Wie Sie sich wahrscheinlich bereits gedacht haben, habe ich die Dinge drastisch vereinfacht. Der echte Intel-8088-Prozessor verwendete aber tatsächlich ähnliche Befehle und einige Hundert weitere.

Es folgen nun einige Beispiele aus der echten Maschinensprache des Intel 8088:

10111010	Bei der nächsten Codezeile handelt es sich um eine Zahl. Speichere diese Zahl im DX-Register.
01000001	Addiere 1 zur Zahl, die sich bereits im CX-Register befindet.
00111100	Vergleiche den Wert im AX-Register mit der nächsten Codezeile.

Wenn wir die Maschinenbefehle, die sogenannten *Codezeilen*, einzeln am externen Datenbus anlegen, können wir dem Schachtelmann bestimmte Aufgaben stellen. Die Gesamtheit der Maschinenbefehle, die eine CPU versteht, wird deren *Befehlssatz* genannt.

Das kann unsere CPU also bisher: Der Schachtelmann kann mit der Außenwelt über den externen Datenbus kommunizieren, hat vier Register und ein Codebuch, mit dem er die verschiedenen am externen Datenbus anliegenden Muster (Befehle in Maschinensprache) verstehen kann (Abbildung 3.8).

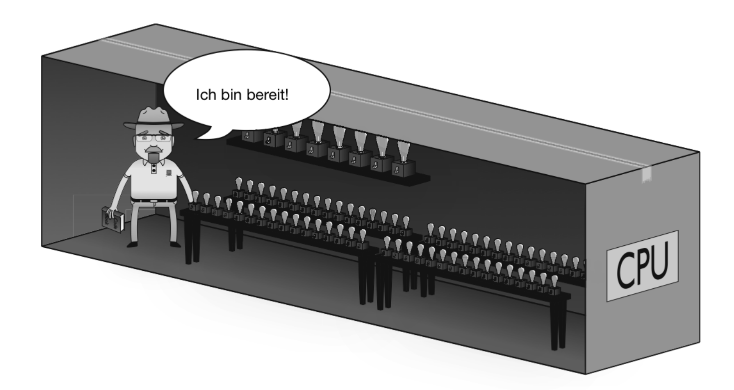


Abb. 3.8: Die CPU bis hierhin

3.1.3 Die Taktleitung

Nun können wir also den Schachtelmann für uns arbeiten lassen. Wir können ihm Daten und Befehle über den externen Datenbus übermitteln. Woher soll er aber wissen, wann eine Aufgabenstellung beendet ist und er an die Arbeit gehen soll?

Stellen Sie sich vor, dass es im Innern der Schachtel eine Klingel gibt, die von außen über einen Knopf betätigt wird. Immer, wenn die Klingel ertönt, liest der Schachtelmann die geschalteten Glühbirnen des externen Datenbusses. Natürlich gibt es in einem echten Computer keine Klingel. Dabei handelt es sich vielmehr um eine spezielle Leitung, die sogenannte *Taktleitung*. (Meist wird die Taktleitung mit *CLK* für engl. Clock bezeichnet.) Wenn an der Taktleitung Spannung anliegt, dann weiß die CPU, dass ein weiterer Satz Daten auf seine Verarbeitung wartet (Abbildung 3.9).

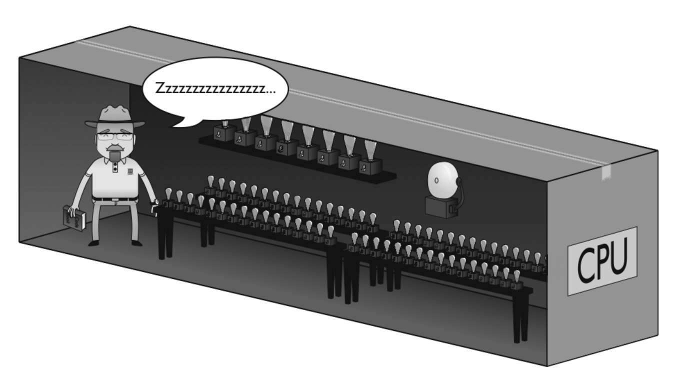


Abb. 3.9: Die CPU macht nichts, bis sie über die Taktleitung aktiviert wird.

Damit die CPU einen am externen Datenbus anliegenden Befehl verarbeitet, muss eine bestimmte Mindestspannung an die Taktleitung angelegt werden. Ein solcher Spannungspuls der Taktleitung

wird *Taktzyklus* genannt. Tatsächlich benötigt die CPU mindestens zwei Taktzyklen zur Verarbeitung eines Befehls, meist jedoch mehr. Bei der manuell bedienten mechanischen Rechenmaschine müsste der Hebel mindestens zweimal gezogen werden, bevor etwas passiert. Tatsächlich gibt es Befehle, für deren Verarbeitung die CPU Hunderte von Taktzyklen benötigt (Abbildung 3.10).

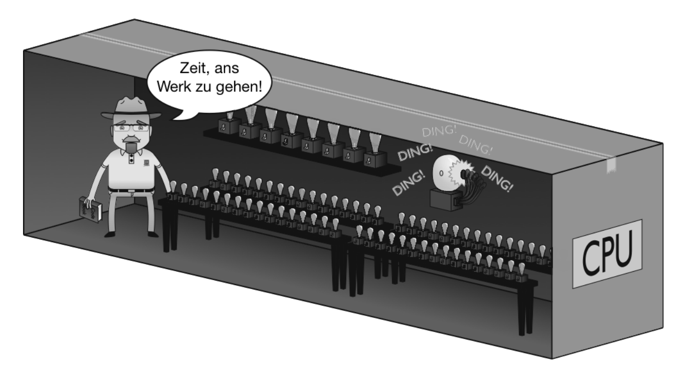


Abb. 3.10: Die CPU benötigt häufig mehr als einen Taktzyklus für eine Aufgabe.

Die maximale Anzahl Taktzyklen, mit der ein Prozessor innerhalb einer bestimmten Zeitspanne umgehen kann, wird *Taktfrequenz* genannt. Dabei handelt es sich um die maximale Arbeitsgeschwindigkeit einer CPU, die vom Prozessorhersteller festgelegt wird. Der Intel 8088 arbeitete ursprünglich mit einer Taktfrequenz von 4,77 MHz (Megahertz; Millionen Arbeitstakte pro Sekunde) und damit nach heutigen Maßstäben extrem langsam. Dennoch handelt es sich verglichen mit Papier und Bleistift immer noch um eine ziemlich hohe Zahl! Moderne Prozessoren arbeiten häufig mit Taktfrequenzen jenseits der 5 GHz (5 Milliarden Arbeitstakte pro Sekunde).

1 Hertz (1 Hz) = 1 Arbeitstakt pro Sekunde

1 Megahertz (1 MHz) = 1 Million Arbeitstakte pro Sekunde

1 Gigahertz (1 GHz) = 1 Milliarde Arbeitstakte pro Sekunde

Sie sollten sich darüber klar sein, dass es sich bei der Taktfrequenz einer CPU um die *maximale* Frequenz handelt, bei der sie noch stabil arbeiten kann, und nicht die Frequenz, mit der sie arbeiten *muss*. Eine CPU eignet sich für alle Taktfrequenzen unterhalb ihres Maximalwerts. Üblicherweise wird die Taktfrequenz direkt auf dem Prozessorgehäuse angegeben (Abbildung 3.11). Andere Modelle verwenden möglicherweise einen kryptischen Code.



Abb. 3.11: Angabe der Taktfrequenz auf einer CPU (3,30 GHz)

Hinweis

Prozessorhersteller bieten exakt dasselbe Prozessormodell mit einer Reihe verschiedener Taktfrequenzen an. Da alle diese Prozessoren aus demselben Fertigungsprozess stammen, stellt sich die Frage nach dem Grund der unterschiedlichen Geschwindigkeiten. Diese rühren daher, dass es zwischen allen CPUs gewisse minimale Unterschiede gibt. Aufgrund von Fertigungstoleranzen bzw. minimalen Fehlern im Silizium, aus dem die Prozessoren gefertigt werden, eignet sich manche Prozessoren besser für höhere Taktfrequenzen als andere. Die unterschiedlichen maximalen Taktfrequenzen der Prozessoren werden bei der Fertigung durch Funktionstests ermittelt.

Der *Quarzbaustein* des Systems entscheidet darüber, mit welcher Systemgeschwindigkeit die CPU und der Rest des Rechners arbeiten. Bei diesem Quarzbaustein handelt es sich in der Regel um einen Quarzoszillator, der dem Schwingquarz in Armbanduhren ähnelt und auf das Mainboard aufgelötet ist (Abbildung 3.12).

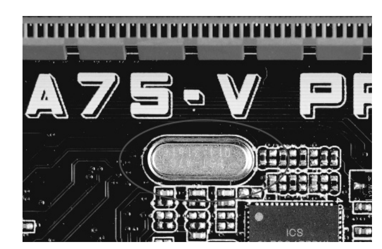


Abb. 3.12: Einer der vielen Typen von Quarzoszillatoren

Der Quarzoszillator gibt mehrere Millionen Mal in der Sekunde einen elektrischen Impuls in einer bestimmten Geschwindigkeit. Dieses Signal erreicht erst einen Taktgeberchip (den *Systemtaktgeber*), der den Takt anpasst und den Quarztakt um ein großes Vielfaches auf den *Systemtakt* anhebt. (Die Hersteller der Mainboards könnten den Quarz auch direkt an die Taktgeberleitung der CPU anschließen, aber wenn man dann die CPU durch eine schnellere oder langsamere ersetzen will, müsste man auch den Quarzbaustein ersetzen.) Solange der PC eingeschaltet ist, sorgt der Quarzoszillator über den Taktgeberchip ständig für die Taktsignale auf der CLK-Leitung und damit dafür, dass das System weiterarbeitet.

Sie können sich den Systemtaktgeber als eine Art Metronom für den Prozessor vorstellen. Während der PC eingeschaltet ist, sorgt der Quarz wiederholt dafür, dass die CLK-Leitung Impulse erhält, und gibt gewissermaßen den Takt für die Aktivitäten des Prozessors vor. Wenn der Systemtaktgeber einen Takt vorgibt, der langsamer als der nominelle Takt des Prozessors ist, dann funktioniert der Prozessor trotzdem tadellos, arbeitet aber nur mit der geringeren Geschwindigkeit des Systemtaktgebers. Wenn der Systemtaktgeber den Prozessor dazu zwingt, mit höherem als seinem nominellen Takt zu arbeiten, dann besteht die Gefahr, dass dieser überhitzt und seine Arbeit einstellt. Bevor Sie eine CPU installieren, müssen Sie sich vergewissern, dass der Systemtaktgeber die richtige Taktfrequenz für die fragliche CPU liefert. Früher musste die Taktfrequenz äußerst sorgfältig abgestimmt werden. Bei heutigen Systemen kommunizieren das Mainboard und die CPU miteinander. Die CPU gibt die erforderliche Taktfrequenz an und der Systemtaktgeber passt sich daran an. Für den Benutzer geht dieser Vorgang unmerklich vonstatten.

Hinweis

Experimentierfreudige Anwender übertakten Prozessoren manchmal bewusst und sorgen dafür, dass der Taktgeberchip einen höheren Multiplikator verwendet und den Takt damit auf eine höhere als die für die CPU vorgesehene Geschwindigkeit anhebt. Das soll langsamere (preiswertere) CPUs beschleunigen, um mit anspruchsvollen Programmen mehr Leistung zu erzielen. Weitere Informationen finden Sie im Abschnitt *Übertakten* später in diesem Kapitel.

3.1.4 Zurück zum externen Datenbus

Und noch ein Praxistest. Bisher ging es um Tische mit Reihen von Glühbirnen. Echte Prozessorregister benutzen natürlich keine Birnen zur Darstellung von An/1 und Aus/0. Register sind winzige Speicherbereiche im Prozessor, mikroskopisch kleine Halbleiterschaltkreise. Wenn einer dieser Schaltkreise eine Ladung trägt, dann entspricht dies einer leuchtenden Lampe. Trägt der Schaltkreis keine Ladung, dann bleibt die Glühbirne aus.

Abbildung 3.13 zeigt das Diagramm eines echten 8088-Prozessors mit den Leitungen des externen Datenbusses und des Taktgebers. Die Register befinden sich im Innern der CPU und sind daher in der Grafik nicht zu sehen.

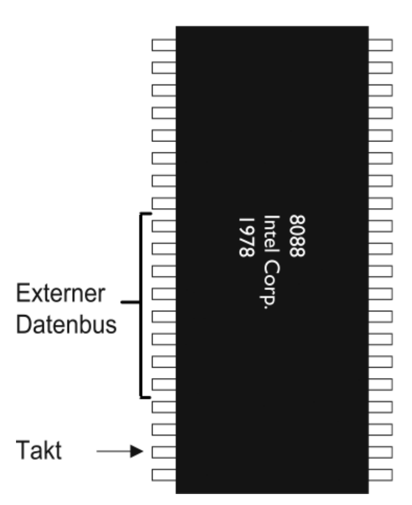


Abb. 3.13: 8088-CPU mit den Leitungen für den externen Datenbus und den Takt

Da Sie nun alle am Vorgang beteiligten Komponenten kennen, können Sie anhand des folgenden einfachen Beispiels probieren, wie diese die CPU arbeiten lassen. In diesem Beispiel fordern Sie die CPU zur Addition von 2 + 3 auf. Dazu müssen Sie der CPU eine Reihe von Befehlen übermitteln, die dann verarbeitet werden, bis Sie schließlich das Ergebnis erhalten. Entnehmen Sie dem Codebuch in Abbildung 3.7, wie Sie die Befehle für den Schachtelmann in ihre Binärform übersetzen müssen.

Haben Sie die Aufgabe zu lösen versucht? So funktioniert es:

1. Legen Sie 10000000 am externen Datenbus (EDB) an.
2. Legen Sie 00000010 am EDB an.
3. Legen Sie 10010000 am EDB an.
4. Legen Sie 00000011 am EDB an.
5. Legen Sie 10110000 am EDB an.
6. Legen Sie 11000000 am EDB an.

Nach Abschluss von Schritt 6 lautet der am EDB anliegende Wert 00000101 und entspricht damit der Dezimalzahl 5 in Binärdarstellung.

Glückwunsch! Sie haben gerade mit den Befehlen aus dem Codebuch die Zahlen 2 und 3 addiert. Derartige Befehlsfolgen, die einem Prozessor in einer bestimmten Reihenfolge übermittelt werden und diesem als Arbeitsanleitung dienen, werden *Programm* genannt. Immer wenn die Leitungen des externen Datenbusses neu gesetzt werden, handelt es sich um eine weitere *Codezeile*. Unser Programmbeispiel besitzt daher sechs Codezeilen.

3.2 Speicher

Mittlerweile wissen Sie, wie Programmcode vom Prozessor ausgeführt wird. Nun blicken wir für einen Augenblick noch einmal zurück und fragen uns, wie der Programmcode auf den externen Datenbus (EDB) gelangt. Das Programm selbst ist auf der Festplatte gespeichert. Theoretisch könnte man Rechner konstruieren, die Daten direkt von der Festplatte zum Prozessor übertragen. Dabei gibt es allerdings ein Problem: Die Festplatte ist zu langsam. Selbst der betagte 8088 mit seiner Taktfrequenz von 4,77 MHz kann jede Sekunde mehrere Millionen Codezeilen verarbeiten. Moderne Prozessoren schaffen mehr als eine Milliarde Zeilen je Sekunde. Festplatten sind für den Prozessor einfach zu langsam.

Computer benötigen andere Geräte, die Kopien der Programme von der Festplatte übernehmen und sie dann zeilenweise zur CPU übertragen, die schnell genug sind, um deren Anforderungen zu erfüllen. Da alle Programmzeilen nichts anderes als Binärmuster sind, würden sich dazu alle Geräte eignen, die Einsen und Nullen speichern können. Geräte, die auf die eine oder andere Weise Nullen und Einsen speichern und auf die eine CPU zugreifen kann, sind allgemein als *Speicher* bekannt.

Viele Arten von Geräten können Binärmuster perfekt speichern, aus technischer Sicht zählt sogar ein Blatt Papier als Speicher, aber Computer benötigen Speicher, der mehr kann, als nur Gruppen aus acht Einsen und Nullen aufzunehmen. Betrachten Sie dazu folgenden Pseudocode:

1. Lege 2 im AX-Register ab.
2. Lege 5 im BX-Register ab.
3. Wenn AX größer als BX ist, führe Zeile 4 aus, andernfalls springe zu Zeile 6.
4. Addiere 1 zum Wert in AX.
5. Gehe zurück zu Zeile 2.
6. Lege den Wert von AX auf dem externen Datenbus ab.

Dieses Programm enthält eine IF-Anweisung, die auch *Sprunganweisung* genannt wird. Die CPU muss jede Zeile des Speichers direkt ansprechen können, um zum Speicher z.B. sagen zu können: »Gib mir die nächste Codezeile« oder »Gib mir Zeile 6.« Die Speicheradressierung löst noch ein anderes Problem: Der Speicher muss nicht nur Programme, sondern auch deren Ergebnisse aufnehmen können. Wenn die CPU 2 + 3 addiert und 5 erhält, muss das Ergebnis so im Speicher abgelegt werden können, dass es später von anderen Programmen gelesen werden kann, oder es muss auf der Festplatte abgespeichert werden. Über die Adresse der Speicherzeile erfahren andere Programme, wo sie die Daten finden können.

3.2.1 Speicher und RAM

Speicher muss nicht nur Programme, sondern auch Daten aufnehmen. Die CPU muss sie vom Speichermedium lesen und darauf schreiben können. Darüber hinaus muss das System der CPU den Sprung zu *beliebigen* Codezeilen ermöglichen, und zwar genau so einfach wie zu anderen gespeicherten Codezeilen. All dies muss zumindest annähernd in der Taktgeschwindigkeit der CPU erfolgen. Glücklicherweise gibt es diese faszinierenden Komponenten schon seit vielen Jahren: *RAM* (*Random Access Memory*). In Kapitel 4, *RAM*, wird das Konzept des Arbeitsspeichers ausführlich erläutert. An dieser Stelle genügt es, wenn Sie sich das RAM als elektronisches Arbeitsblatt einer Tabellenkalkulation vorstellen, wie Sie es z.B. mit Microsoft Excel erstellen können (Abbildung 3.14). Jede Zelle in dieser Tabelle kann lediglich eine Eins oder eine Null speichern. Eine einzelne Zelle wird *Bit* genannt. Jede Zeile in der Tabelle ist 8 Bit breit, um dem externen Datenbus beim 8088 zu entsprechen. Jede Zeile mit jeweils 8 Bit wird *Byte* genannt. Beim PC werden Daten zwischen RAM und Prozessor in ein Byte großen Blöcken übertragen. Das RAM ist daher in Bytezeilen organisiert. Die folgenden Begriffe werden im Zusammenhang mit Bits verwendet:

- Eine einzelne Eins oder Null = 1 Bit
- 4 Bit = 1 Nibble
- 8 Bit = 1 Byte
- 16 Bit = 1 Wort
- 32 Bit = 1 Doppelwort
- 64 Bit = 1 Quadword

1	0	0	0	0	0	1	1
0	1	0	0	0	0	0	0
0	0	0	0	1	1	0	1
0	1	0	1	0	0	0	0
0	0	0	0	0	0	0	1
0	1	0	1	1	0	1	0
0	0	1	1	1	1	0	0
0	0	0	0	1	0	0	1
1	1	1	0	0	0	0	0
0	0	1	0	1	1	1	0
1	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0

Abb. 3.14: Aus der Sicht der CPU stellt das RAM eine Tabelle dar.

Die Anzahl der RAM-Zeilen ist von PC zu PC unterschiedlich. Zwischen 1980 und 1990 verfügte ein typischer PC nur über einige Hunderttausend Byte RAM. Die heutigen Systeme haben dagegen oft zig Milliarden Byte RAM.

Betrachten wir nun einmal kurz die Realität. Aus elektronischer Sicht ähnelt RAM dem Arbeitsblatt einer Tabellenkalkulation, aber das echte RAM besteht aus Gruppen von Halbleiterchips, die auf kleine Platinen gelötet sind, die in Ihren Computer eingesetzt werden (Abbildung 3.15). In Kapitel 4, *RAM*, erfahren Sie, wie diese Chipgruppen es schaffen, wie ein Arbeitsblatt auszusehen. Hier sollten Sie sich noch keine weiteren Gedanken über echtes RAM machen und weiter an das Arbeitsblatt einer Tabellenkalkulation denken.

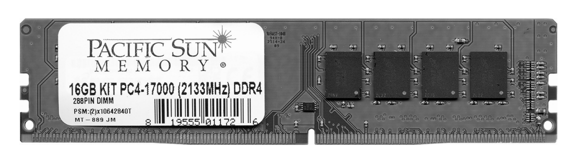


Abb. 3.15: Typischer RAM-Baustein

Der Begriff *wahlfreier Zugriff* (engl. *Random Access*) bedeutet, dass die CPU auf alle Zeilen im RAM schnell und nach Belieben zugreifen kann. Auf das RAM kann nicht nur wahlfrei (direkt auf beliebige Speicherstellen) zugegriffen werden, sondern es ist auch schnell. Durch Speicherung der Programme im RAM kann der Prozessor sehr schnell auf sie zugreifen und sie ausführen. Im RAM werden außerdem die aktuell vom Prozessor genutzten Daten gespeichert.

Computer verwenden für den Hauptspeicher des Systems *dynamisches RAM* (*DRAM*). DRAM benötigt sowohl eine konstante elektrische Ladung als auch eine regelmäßige Auffrischung der Schaltkreise, sonst gehen die Daten verloren, weshalb es hinsichtlich seines Inhalts eben dynamisch und nicht statisch ist. Die Auffrischung kann Verzögerungen verursachen, weil die CPU auf deren Abschluss warten muss. Die Hersteller moderner CPUs haben aber intelligente Verfahren entwickelt, um dies zu kompensieren, wie Sie später in diesem Kapitel noch erfahren werden, wenn es um die verschiedenen Prozessorgenerationen geht.

Verwechseln Sie das RAM nicht mit Massenspeichern wie Festplatten und Flash-Laufwerken, die der dauerhaften Speicherung von Programmen und Daten dienen. Der permanente Speicher wird in den Kapiteln 8 bis 10 eingehender beschrieben.

3.2.2 Adressbus

Bis jetzt besteht unser PC nur aus einem Prozessor und RAM. Was wir jetzt noch brauchen, ist eine Art Verbindung zwischen der CPU und dem RAM, die dafür sorgt, dass beide miteinander kommuni-

zieren können. Dazu werden wir den externen Datenbus des Prozessors so erweitern, dass der Prozessor mit dem RAM kommunizieren kann (Abbildung 3.16).

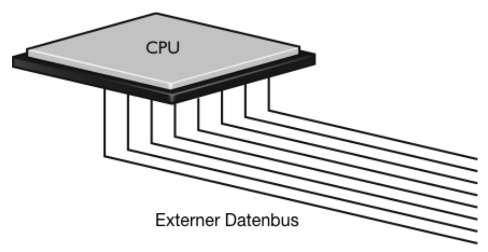


Abb. 3.16: Externer Datenbus

Denken Sie nun einmal nach – auf welche Weise lässt sich das RAM mit dem externen Datenbus verbinden? Nur Zusammenstecken reicht ja nicht! Das RAM ist eine Tabelle mit Tausenden und Abertausenden einzelner Zeilen, während zu einem gegebenen Zeitpunkt immer nur der Inhalt einer Zeile betrachtet werden soll. Wie kann man die Sache also angehen? Wie kann das RAM so mit dem externen Datenbus verbunden werden, dass der Prozessor jede beliebige Zeile sehen und dabei weiterhin alle Zeilen im RAM erreichen kann?

Wir brauchen irgendeinen Chip zwischen dem RAM und der CPU, der die Verbindung herstellt. Die CPU muss angeben können, welche RAM-Zeile sie benötigt, und der Chip sollte sich um die Einzelheiten kümmern und wissen, wie er genau diese Datenzeile aus dem RAM holen und auf dem externen Datenbus ablegen kann. Dieser Chip wird unterschiedlich bezeichnet, aber hier werde ich ihn jedenfalls *MCC* (*Memory Controller Chip*, *dt. Speicher-Controller-Chip*) nennen.

Der MCC enthält spezielle Schaltkreise, mit deren Hilfe er den Inhalt jeder RAM-Zeile übernehmen und Daten oder Befehle auf dem externen Datenbus ablegen kann. Damit kann die CPU wiederum diesem Code entsprechend agieren (Abbildung 3.17).

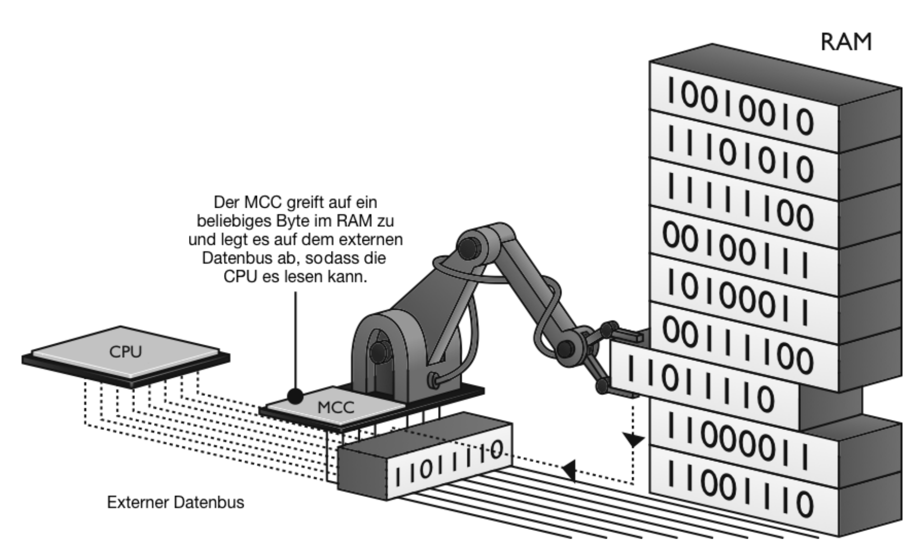


Abb. 3.17: Der MCC holt ein Byte aus dem RAM.

Wenn der MCC seinen Platz eingenommen hat und beliebige Bytes aus dem RAM holen kann, muss die CPU dem MCC noch mitteilen können, welche Codezeile sie benötigt. Die CPU erhält daher einen zweiten Satz Leitungen, der Adressbus genannt wird, über den sie mit dem MCC kom-

munizieren kann. Unterschiedliche CPUs nutzen unterschiedlich viele Leitungen (und Sie werden gleich sehen, dass dies von größter Bedeutung ist). Beim 8088 besaß der Adressbus 20 Leitungen (Abbildung 3.18).

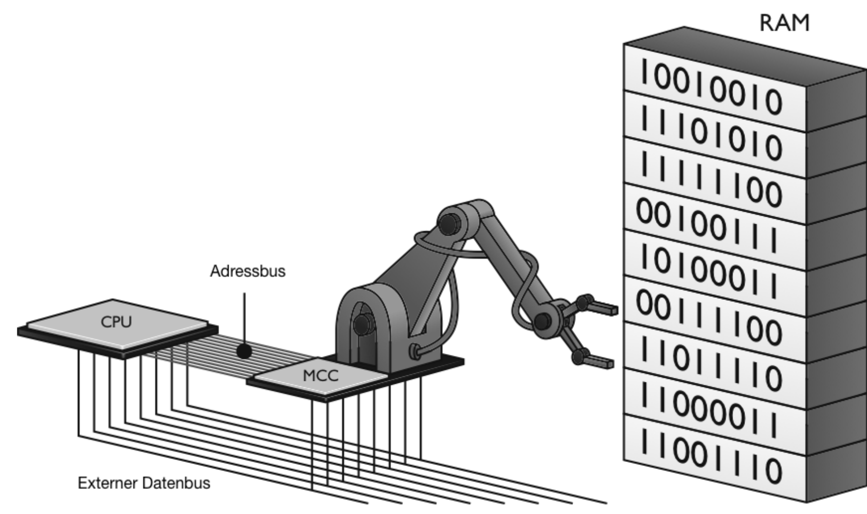


Abb. 3.18: Der Adressbus

Durch Aktivierung und Deaktivierung der Adressbusleitungen teilt die CPU dem MCC mit, welche Zeile aus dem RAM sie gerade benötigt. Jedes einzelne Muster aus Einsen und Nullen auf diesen 20 Leitungen verweist genau auf ein Byte RAM. Damit stellen sich zwei wichtige Fragen. Erstens, wie viele verschiedene Muster aus aktivierten/deaktivierten Leitungen gibt es bei 20 Leitungen? Und zweitens, welches Muster bezieht sich auf welche RAM-Zeile?

Wie viele Muster?

Die Antwort auf die erste Frage lässt sich mit ein wenig einfacher Rechnerei leicht ermitteln: Jede Leitung hat entweder den Zustand Ein oder Aus und kann daher nur zwei unterschiedliche Zustände annehmen: Ein oder Aus. Wenn der Adressbus aus nur einer einzigen Leitung bestünde, könnte diese Leitung jeweils nur entweder Ein oder Aus sein. Rechnerisch ergibt dies $2^1 = 2$ verschiedene Kombinationsmöglichkeiten. Gibt es dagegen zwei Adressbusleitungen, sind es bereits $2^2 = 4$ verschiedene Kombinationen. Bei 20 verschiedenen Leitungen ergeben sich 2^{20} (bzw. 1.048.576) verschiedene Kombinationen. Da jedes Muster auf eine Zeile Code verweist und jede RAM-Zeile ein Byte enthält, kennen Sie daher mit der Anzahl der Leitungen im Adressbus gleichzeitig die Maximalgröße des Arbeitsspeichers, die eine bestimmte CPU verwalten kann.

Da der 8088-Adressbus aus 20 Leitungen bestand, konnte er maximal 2^{20} bzw. 1.048.576 Byte verwalten und besaß damit einen *Adressraum* von 1.048.576 Byte. Das heißt aber nicht, dass jeder Computer mit einer 8088-CPU 1.048.576 Byte RAM besaß – weit gefehlt! Der Original-IBM-PC war nur mit 64 Kilobyte ausgestattet – und das hielt man am Anfang des Computerzeitalters in den frühen 1980ern für mehr als ausreichend.

Sie wissen nun also, dass der 8088 über 20 Adressleitungen und einen Adressraum von 1.048.576 Byte verfügte. Das stimmt zwar, aber niemand verwendet diese Zahlen, wenn es um den Adressraum des 8088 geht. Stattdessen sagt man, dass der Adressraum des 8088 ein *Megabyte* (1 MB) groß ist.

Was ist ein »Mega«? Befassen wir uns also ein wenig mit der Terminologie. Wenn wir es mit Computern zu tun haben, dann haben wir es ständig mit der Anzahl der Muster zu tun, die über einen Satz Leitungen dargestellt werden können. Bestimmte Zweierpotenzen haben daher Bezeichnungen, die im Rechnerbereich häufig verwendet werden. Diese werden in der folgenden Aufstellung erläutert:

- 1 Kilo (K) = 2^{10} = 1.024
- 1 Kilobyte (KB) = 1.024 Byte
- 1 Mega (M) = 2^{20} = 1.048.576
- 1 Megabyte (MB) = 2^{20} = 1.048.576 Byte
- 1 Giga (G) = 2^{30} = 1.073.741.824
- 1 Gigabyte (GB) = 2^{30} = 1.073.741.824 Byte
- 1 Tera (T) = 2^{40} = 1.099.511.627.776
- 1 Terabyte (TB) = 1.099.511.627.776 Byte
- Metrisches System und Arbeitsspeicher

Mit der obigen Liste gibt es ein Problem. Wenn Sie sich mit einem Experten für das metrische System unterhalten, werden Sie zu hören bekommen, dass ein Kilo gleich 1.000 ist, nicht 1.024! Habe ich also gelogen? Nun ja, tatsächlich, aber nicht aus Bosheit. Ich überbringe lediglich die Nachricht. Vor geraumer Zeit geschah Folgendes:

In der Frühzeit des Computers entstand die Notwendigkeit für Bezeichnungen großer Werte, aber die Wörter gab es noch nicht. In einem Fall versuchte man, Werte zu verwenden, die wie gerade beschrieben auf Zweierpotenzen beruhen. Aber niemand hatte sich Bezeichnungen für 1.024 oder 1.048.576 ausgedacht, also verwendete man einfach Kilo und Mega, weil 1.000 nah genug an 1.024 und 1.000.000 nah genug an 1.048.576 war.

Unterdessen wurden für die Geschwindigkeit von Prozessoren und die Größe von Festplatten jedoch keine auf Zweierpotenzen beruhenden Werte verwendet. Man benutzte einfach 1.000 für Kilo und 1.000.000 für Mega.

Von Anfang der 1980er-Jahre bis etwa 1990 war es den Leuten egal, dass es zwei verschiedene Zählweisen gab. Alles war in Ordnung, bis die Mathefreaks und Rechtanwälte damit anfingen, Ärger zu machen. Um dem ein Ende zu bereiten, stellte das IEC (International Electrotechnical Comittee) 1998 spezielle Präfixe für Binärwerte vor, die ich als »Ibis« bezeichne:

- 1 Kibi (Ki) = 2^{10} 1.024 Byte
- 1 Mebi (Mi) = 2^{20} = 1.048.576 Byte
- 1 Gibi (Gi) = 2^{30} = 1.073.741.824 Byte
- 1 Tebi (Ti) = 1.099.511.627.776 Byte

Um der neuen Namenskonvention Rechnung zu tragen, sollten Sie also sagen: »Der 8088 konnte ein Mebibyte (MiB) Arbeitsspeicher adressieren.« Das Problem ist nur, dass außer den Mathefreaks *niemand* die Ibis verwendet. Die RAM-Hersteller verwenden den Begriff Gigabyte, obwohl sie technisch gesehen den Begrif Gibibyte verwenden müssten. Willkommen in der merkwürdigen Welt der Zählweise in der IT. Aber nun zurück zum RAM.

Welches Muster entspricht welcher Zeile?

Die zweite Frage ist etwas schwieriger zu beantworten: »Welches Muster entspricht welcher Zeile im RAM?« Um diese Frage zu verstehen, müssen Sie zuvor ein wenig über Binärzahlen wissen. Im Binärsystem existieren nur die beiden Zahlen 0 und 1, daher eignet es sich besonders gut für die Darstellung der beiden möglichen Leitungszustände Ein und Aus. Versuchen Sie einmal, binär zu zählen: 0, 1 ... und was kommt dann? Jedenfalls nicht 2 – Sie können nur 0 und 1 verwenden! Die nächste Zahl nach 1 ist 10! Versuchen Sie nun einmal binär bis 1.000 zu zählen: 0, 1, 10, 11, 100, 101, 110, 111, 1000. Probieren Sie einmal, bis 10.000 zu zählen, und seien Sie unbesorgt, denn Sie werden dafür nicht lange brauchen!

Ihre neuen binären Kenntnisse können Sie nun mit dem vorgestellten Konzept verknüpfen. Gehen Sie nun von binär wieder zur guten alten dezimalen Zählweise (zur Basis 10) zurück – nehmen Sie an, dass Sie die Zahl 365 haben, der Sie Nullen voranstellen, etwa so: 000365. Am Wert der Zahl ändert

sich dadurch nichts. Zählen Sie jetzt noch einmal binär und fügen Sie auf die beschriebene Weise so viele Nullen hinzu, dass 20 Stellen entstehen:

```
00000000000000000000
00000000000000000001
00000000000000000010
00000000000000000011
00000000000000000100
00000000000000000101
00000000000000000110
00000000000000000111
00000000000000001000
```

Das wäre doch eine großartige Möglichkeit zur Darstellung der RAM-Zeilen auf dem Adressbus, oder etwa nicht? Die CPU würde das erste Byte im RAM auf dem Adressbus über 000000000000000 00000 erkennen. Die letzte RAM-Zeile erhält für die CPU die Adresse 11111111111111111111. Wenn die CPU alle Adressbusleitungen ausschaltet, will sie also die erste RAM-Zeile lesen, schaltet sie dagegen alle Leitungen ein, geht es um die 1.048.576ste RAM-Zeile. Natürlich lassen sich so auch alle RAM-Zeilen dazwischen über den Adressbus ansprechen. Über die verschiedenen Muster aus Einsen und Nullen auf dem Adressbus kann der Prozessor also auf beliebige Zeilen im Speicher zugreifen.

Hinweis

Bits und Bytes werden unterschiedlich abgekürzt. Der *Groß*buchstabe B steht abkürzend für Byte, während der *Klein*buchstabe b abkürzend für Bit steht. Bei 4 KB handelt es sich also um vier Kilobyte, während 4 Kb für vier Kilobit steht! Dieser Standard gilt auch für die anderen Bezeichnungen: 2 Mb = 2 Megabit, 2 MB = 2 Megabyte, 4 Gb = 4 Gigabit, 4 GB = 4 Gigabyte usw.

1001

3.3 Moderne Prozessoren

Die Hersteller haben seit den Tagen des Intel 8088 erstaunliche Fortschritte bei den Prozessoren erzielt, die aber noch immer auf dieselbe Weise wie ihr Urahn funktionieren. Noch immer führt die *ALU* (*Arithmetic Logic Unit*), also unser Freund, der Schachtelmann, Abermillionen von Berechnungen pro Sekunde aus. Dabei muss der Speicher den CPUs die Codezeilen schnellstmöglich bereitstellen.

Dieser Abschnitt bietet einen Überblick über den modernen Prozessormarkt. Zunächst werden wir die heute verfügbaren Prozessorgenerationen betrachten, danach wenden wir uns entscheidenden Verbesserungen der Technologie zu, deren Bedeutung Sie verstehen sollten.

3.3.1 Hersteller

Als IBM 1980 Intel anbot, CPUs für ihren neuen IBM PC zu liefern, entstand für Intel damit mehr oder weniger ein Monopol für alle PC-CPUs. Die anderen CPU-Hersteller dieser Zeit wurden immer unwichtiger: MOS Technology, Zilog, Motorola – keiner konnte direkt mit Intel konkurrieren. Mit der Zeit entstanden andere Konkurrenten, die Intel die Vorherrschaft in diesem Marktbereich streitig machen. Insbesondere das Unternehmen *AMD* (*Advanced Micro Devices*) begann, Nachbauten der Intel-CPUs herzustellen, womit ein interessanter und ziemlich halsabschneiderischer Wettbewerb mit Intel entstand, der bis heute andauert.

Hinweis

Die ständig wachsende Auswahl mobiler Geräte, wie z.B. Apples iPhone und iPad, nutzen eine von der Firma ARM Holdings entwickelte Prozessorarchitektur, die den Namen *ARM* trägt. ARM-Prozessoren verwenden ein einfacheres, energiesparenderes Design, die RISC-Architektur (*Reduced Instruction Set Computing*, ein vereinfachter Befehlssatz). ARM-Prozessoren sind zwar nicht ganz so leistungsfähig wie die CISC-Chips (*Complex Instruction Set Computing*) von Intel und AMD, sie sind aber aufgrund des günstigen Preises und des niedrigen Stromverbrauchs für mobile Geräte ideal.

(Beachten Sie hier, dass eine klare Unterscheidung zwischen RISC- und CISC-Architektur zunehmend schwieriger wird. Beide Architekturen übernehmen heutzutage Features der jeweils anderen, um effizienter zu arbeiten.)

ARM Holdings entwirft die ARM-CPUs, stellt sie aber nicht selbst her. Viele andere Unternehmen, vor allem Qualcomm, lizenzieren das Design und produzieren ihre eigenen Versionen. In Kapitel 24, *Mobile Geräte*, erfahren Sie mehr über ARM-Prozessoren.

Intel

Intel hat den PC-Markt mit seinen Prozessoren und Mainboard-Chipsätzen weitgehend dominiert. An fast jedem einzelnen Schritt in der Entwicklung des Personal Computers war Intel wegweisend mit technologischen Fortschritten und einer – für ein derart großes Unternehmen – erstaunlichen Flexibilität beteiligt. Intel-Prozessoren und deren Befehlssätze definieren den Personal Computer. Intel stellt aktuell rund ein Dutzend Prozessormodelle für Desktop-Rechner, Laptops und Notebooks her, die Markennamen wie *Core*, *Pentium* oder *Celeron* tragen. Die Prozessoren für die leistungsstärksten Workstations/Server wurden Xeon getauft.

AMD

Advanced Micro Devices (AMD) stellt hervorragende Prozessoren für den PC-Markt her und bleibt Intel auf dem Prozessormarkt seit etlichen Jahren dicht auf den Fersen. Wie Intel stellt auch AMD nicht nur Prozessoren her. Der Prozessorbereich ist aber sicherlich der Bereich, von dem öffentlich am meisten Notiz genommen wird. AMD hat Prozessoren hergestellt, die die Funktion der Intel-CPUs nachgebildet haben (Klone). Wenn Intel den im Original-IBM-PC verwendeten Prozessor erfunden hat, wie konnte AMD dann CPUs nachbauen, ohne verklagt zu werden? Das liegt daran, dass Chiphersteller Technologien gewöhnlich untereinander austauschen und entsprechende gegenseitige Lizenzvereinbarungen treffen. In grauer Vorzeit haben AMD und Intel 1976 eine solche Vereinbarung unterzeichnet, die AMD das Recht zum Kopieren bestimmter Prozessortypen einräumt.





Abb. 3.19: Identische Intel- und AMD-486er von Anfang der 1990er-Jahre

Der Ärger begann mit dem Intel 8088. Intel war bei der Herstellung von CPUs auf AMDs Hilfe angewiesen, um die große Nachfrage von IBM befriedigen zu können. Nach ein paar Jahren war Intel aber enorm gewachsen und wollte nicht mehr, dass AMD Prozessoren fertigte. AMD berief sich auf die

unterzeichnete Vereinbarung und stellte während der 1980er- und bis in die 1990er-Jahre hinein Pin für Pin identische Prozessoren her, die genau den Intel-Prozessor-Produktlinien entsprachen (Abbildung 3.19). Damals konnte man eine Intel-CPU aus einem System ausbauen und sie problemlos durch einen AMD-Prozessor ersetzen!

Nach jahrelangem Rechtsstreit legten Intel und AMD diesen im Januar 1995 bei und einigten sich darauf, das Lizenzabkommen zu beenden. Aufgrund dieses Abkommens sind AMD-Chips nicht mehr mit den Sockeln und Mainboards von Intel kompatibel, auch wenn sie manchmal ähnlich aussehen. Wenn Sie heute einen AMD-Prozessor verwenden wollen, dann müssen Sie auch ein für AMD-Prozessoren entwickeltes Mainboard kaufen bzw. einsetzen. Und wenn Sie einen Intel-Prozessor verwenden wollen, dann müssen Sie auch ein dafür entwickeltes Mainboard benutzen. Sie haben daher zwei Alternativen: Intel oder AMD.

Modellbezeichnungen

Intel und AMD verwenden für ihre Produktreihen verschiedene Bezeichnungen, die sich über die Jahre geändert haben. Intel nutzte viele Jahre lang die Marke *Pentium* für das Spitzenmodell und wechselte bei neuen Prozessorgenerationen nur die Modellnummer: Pentium, Pentium II, Pentium III usw. AMD verwendete die Marke *Athlon* auf ähnliche Weise.

Bei den meisten Diskussionen über CPUs geht es um vier Marktsegmente für die Endprodukte: Desktop-PCs, Einstiegsmodelle, tragbare Computer und Server. In Tabelle 3.1 sind einige der aktuellen Produktlinien und deren Bezeichnungen zusammengefasst.

Marktsegment	Intel	AMD
Enthusiasten	Core i7/i9	Ryzen, Ryzen Threadripper
Standardmodelle	Core i7/i5/i3	A-Reihe Pro, Ryzen
Einstiegsmodelle	Pentium, Celeron	A-Reihe, FX
Tragbare Geräte	Core i7/i5/i3 (mobil), Celeron (mobil)	Ryzen, A-Reihe
Server	Xeon	Opteron, EPYC
Workstation	Xeon	Ryzen Pro, Ryzen Threadripper

Tabelle 3.1: Aktuelle Intel- und AMD-Produktreihen

Sie werden bemerkt haben, dass sowohl Intel als auch AMD die Modellbezeichnungen für Produkte, die auf andere Marktsegmente zielen, wiederverwenden. Der frühere Pentium zielte beispielsweise auf den Markt für Premiummodelle, heutzutage nutzt Intel die Marke für Einstiegsmodelle. Gleiches gilt für die Marke Athlon. Und um die Verwirrung zu vervollständigen, handelt es sich bei den Modellen für den Einstiegsmarkt nicht um die alten CPUs, sondern um Versionen der aktuellen Modellreihe für das untere Marktsegment.

Mikroarchitektur

Intel und AMD entwickeln kontinuierlich schnellere und leistungsfähigere CPUs. Etwa alle drei Jahre stellen sie ein grundlegend neues Design vor, das als Mikroarchitektur bezeichnet wird. Sie versuchen aber gleichzeitig, die Anzahl der in Gebrauch befindlichen Modellbezeichnungen möglichst gering zu halten. Das bedeutet, dass CPUs mit identischer Modellbezeichnung auf den Markt kommen, obwohl sich die CPU deutlich von Vorgängermodellen unterscheidet. Beide Hersteller verwenden daher *Codenamen*, um die unterschiedlichen Varianten innerhalb einer Modellreihe zu kennzeichnen (Abbildung 3.20 Als Techniker müssen Sie sowohl die Modellbezeichnung als auch den Codenamen kennen, um Ihren Kunden angemessene Kaufempfehlungen geben zu können. Dass dieses Wissen unerlässlich ist, illustriert beispielsweise der Intel Core i7.

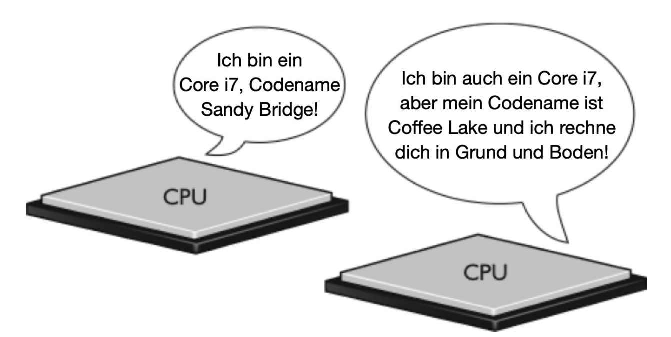


Abb. 3.20: Gleiche Markenbezeichnung, aber verschiedene Fähigkeiten

Intel hat den ersten Core i7 im Sommer 2008 vorgestellt. Bis Anfang 2012 hat die ursprüngliche Mikroarchitektur (mit dem Codenamen Nehalem) fünf verschiedene Varianten durchlaufen, von denen nicht eine einzige mit einem Mainboard funktioniert, das für eine der anderen Varianten entworfen wurde. Darüber hinaus hat Intel im Sommer 2011 die Core-i7-Version mit Sandy Bridge vorgestellt, von der es Varianten für Desktops und tragbare Computer gibt, die natürlich durchweg verschiedene Sockel verwenden. Seitdem hat es jedes Jahr einen neuen Core i7 mit verbesserter Architektur gegeben, die Codenamen wie Ivy Bridge, Haswell, Broadwell usw. trugen. (Und ich vereinfache die Variantenbildung hier noch.)

Hinweis

Die *Prozessorkennung* ist beim Vergleich von Prozessoren äußerst hilfreich, wenn Ihnen die Bedeutung bekannt ist. Bevor wir diese Kennung näher betrachten, müssen jedoch noch einige andere Dinge über Prozessoren zur Sprache kommen. Weitere Informationen finden Sie im Abschnitt 3.4.1, *Auswahl des Prozessors*, später in diesem Kapitel.

Hier schlagen nun viele neue Techniker die Hände über dem Kopf zusammen. Wie soll man da Schritt halten? Wie kann man feststellen, welche CPU das beste Preis-Leistungs-Verhältnis für die Einsatzzwecke Ihrer Kunden bietet? Einfach ausgedrückt: Sie müssen sehr gründlich recherchieren.

Erste Anlaufstelle sind hier die Internetauftritte der Hersteller. Beide Unternehmen stellen eine Menge Informationen zu ihren Produkten bereit.

- `www.intel.com`
- `www.amd.com`

Es gibt außerdem viele technische Webseiten von hoher Qualität, die sich den neuesten CPUs widmen. Wenn einer Ihrer Kunden aufrüsten möchte, recherchieren Sie im Internet und suchen Sie aktuelle Artikel und Vergleichstest. Da Sie die zugrunde liegende Technik dank Ihrer CompTIA A+-Studien beherrschen, wird es Ihnen leichtfallen, der Diskussion zu folgen. Ich besuche regelmäßig folgende Websites:

- `www.arstechnica.com`
- `www.anandtech.com`
- `www.tomshardware.com`
- `www.bit-tech.net`

Und schließlich finden Sie großartige, erschöpfende Artikel über alle möglichen Technikthemen bei Wikipedia:

- `www.wikipedia.org`

Hinweis

Wikipedia ist eine von Benutzern erstellte Ressource, die sich selbst reglementiert. Ich habe festgestellt, dass Wikipedia in technischen Fragen im Allgemeinen sehr zuverlässig ist. Dessen ungeachtet sollten Sie stets auch eine weitere Quelle konsultieren. Die meisten Autoren der Artikel verraten Ihnen in den Fußnoten freundlicherweise ihre eigenen Quellen. Oftmals lassen sich Wikipedia-Artikel auch als eine Art Sprungbrett für weiterführende Suchen nutzen.

Desktop vs. mobiles Gerät

An mobile Geräte, wie tragbare Computer, werden andere Anforderungen als an einen Desktop-Rechner gestellt. Insbesondere sollten diese nur ein Minimum an Energie verbrauchen, denn das bietet zwei Vorteile: Der Akku hält länger und es entsteht weniger Wärme.

Sowohl bei Intel als auch bei AMD arbeiten Ingenieure an der Entwicklung ausgezeichneter Mobilversionen ihrer CPUs, die erweiterte Möglichkeiten zum Energiesparen mitbringen (Abbildung 3.21). Beispielsweise kann die CPU in einem Stromsparmodus arbeiten und automatisch »aufdrehen«, wenn der Anwender mehr Leistung vom Prozessor verlangt. Wenn Sie am Flughafen ein wenig im Internet unterwegs sind, benötigt die CPU nicht besonders viel Energie. Wechseln Sie aber stattdessen zu einem grafisch aufwendigen Spiel, legt auch die CPU einen Gang zu. Energiesparen durch langsamere Taktung der CPU bei vermindertem Bedarf an Rechenleistung nennt man auch *Drosselung* oder *Throttling*.



Abb. 3.21: Desktop vs. mobiles Gerät: Gebt es euch!

Leider wird die ganze Sache komplizierter, wenn man die Wärmeentwicklung betrachtet. Da die meisten tragbaren Computer äußerst kompakt sind, können sie die Wärme nicht so schnell abführen wie ein gut gekühltes Desktop-System. Mobile CPUs können hochgetaktet werden, um anspruchsvolle Aufgaben zu erledigen, werden dann aber schnell sehr warm. Da dabei Temperaturen erreicht werden, bei denen die CPU Schaden nimmt, wird der Prozessor gedrosselt. Ein System, das versucht, anspruchsvolle Aufgaben mit einem Bruchteil seiner verfügbaren Leistung auszuführen, kann fast zum Stillstand kommen!

Hinweis

Wie viel Wärme ein ausgelasteter Prozessor erzeugt, wird durch eine Kennzahl (angegeben in Watt) beschrieben, die man als TDP (*Thermal Design Power*, thermische Verlustleistung) bezeichnet. Die TDP vermittelt Ihnen eine grobe Vorstellung davon, wie viel Energie eine CPU benötigt und welche Kühlung erforderlich ist. Sie ist außerdem bei der Auswahl effizienterer CPUs hilfreich.

Bei der TDP gibt es einen Abwärtstrend (insbesondere in den letzten Jahren), sie vermittelt jedoch einen Eindruck davon, wie diese Werte in der Praxis aussehen. Die TDP der CPUs von Smartphones oder Tablets liegt typischerweise zwischen 2 und 15 Watt, die CPUs von Laptops kommen auf 7 bis 65 Watt und die CPUs von Desktops auf 50 bis 140 Watt.

Viele der für Mobilprozessoren entwickelten Technologien haben auch ihren Weg in die leistungshungrigeren Prozessoren der Desktop-Rechner gefunden, und das ist ein Zusatznutzen für den ganzen Planeten (und senkt Ihre Stromrechnung).

3.3.2 Technologie

Auch wenn die heutigen Mikroprozessoren dem gleichen Zweck dienen wie der altehrwürdige 8088, nämlich dem Durchführen von Berechnungen, so geschieht das doch auf ungleich rationellere Weise. Die CPUs wurden von den Ingenieuren auf vielfältige Art verändert, erweitert und verbessert. In diesem Abschnitt werfen wir einen Blick auf die folgenden acht Merkmale:

- Taktvervielfachung
- 64-Bit-Architektur
- Unterstützung für Virtualisierung
- Parallelverarbeitung
- Mehrkernprozessoren
- Integrierter Memory Controller (IMC)
- Integrierte GPU (*Graphics Processing Unit*)
- Sicherheit

Taktvervielfachung

Alle modernen CPUs laufen mit einem Vielfachen des Systemtakts. Der Systembus meiner Ryzen-7-Maschine ist beispielsweise mit 100 MHz getaktet. Es findet eine bis zu 32-mal vervielfachte Taktung statt (Multiplikator 32), um die maximale Prozessorgeschwindigkeit von 3,2 GHz auszureizen. Ursprünglich wurden die CPUs mit der Geschwindigkeit des Systembusses betrieben, allerdings bemerkten die Ingenieure schon bald, dass die meiste Zeit ausschließlich die CPU irgendwelche Arbeit verrichtete. Wenn man nur die interne Geschwindigkeit der CPU erhöhen könnte und alles andere unverändert lässt, hätte man dennoch insgesamt an Geschwindigkeit hinzugewonnen. Abbildung 3.22 zeigt ein raffiniertes Programm namens *CPU-Z*, das alle Einzelheiten meiner CPU anzeigt. Beachten Sie, dass ich im Augenblick nur diesen Text schreibe und die CPU daher die Taktvervielfachung auf den Multiplikator 16 gedrosselt hat, sodass die Geschwindigkeit der CPU nur 1.546 MHz beträgt.

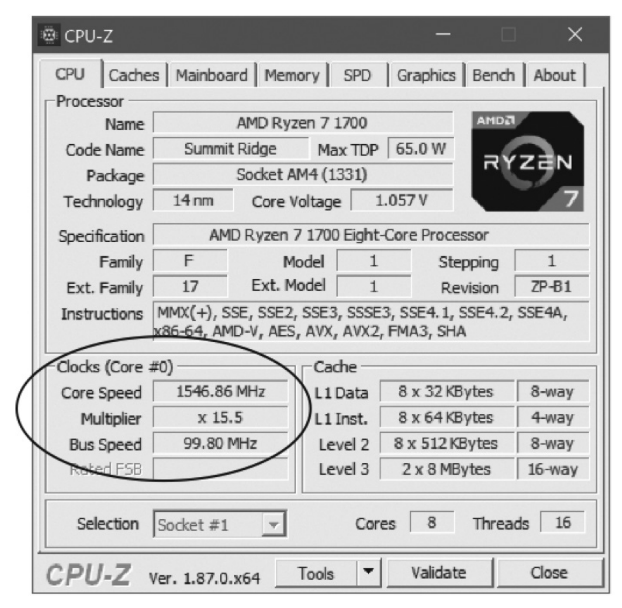


Abb. 3.22: CPU-Z zeigt den Systemtakt, Multiplikator und Systembustakt eines Ryzen-7-Prozessors an, der nicht gerade ins Schwitzen gerät.

Tipp

Stellen Sie sich vor, dass Sie sich in einem Büro voller PCs befinden, die Ihnen nicht vertraut sind. Es gibt keinerlei Dokumentation, daher weist Ihr Chef Sie an, schnellstmöglich so viel wie möglich über die verschiedenen PCs herauszufinden. Probieren Sie es aus: Laden Sie sich eine Kopie des äußerst populären, kostenlosen Programms CPU-Z von `www.cpuid.com` herunter. CPU-Z liefert Ihnen alle erdenklichen Informationen über die CPU. Kopieren Sie das Programm auf einen USB-Stick, den Sie an den verschiedenen Computern einstecken können. (Natürlich nur, wenn Ihnen das gestattet wurde.) Welchen Prozessortyp besitzt der Computer Ihres Nachbarn? Was lässt sich über die Fähigkeiten der verschiedenen Geräte aussagen?

Die Systembusgeschwindigkeit und der Multiplikator mussten bei älteren Systemen mit Taktvervielfachung über kleine Steckbrücken (Jumper) oder DIP-Schalter auf dem Mainboard manuell eingestellt werden (Abbildung 3.23). Moderne Prozessoren teilen dem Mainboard über eine Funktion namens CPUID (CPU Identifier) ihre Kenndaten mit, sodass Systembusgeschwindigkeit und Multiplikator automatisch eingestellt werden. (Bei vielen Mainboards können Sie diese Automatik abschalten. Einzelheiten hierzu finden Sie im Abschnitt *Übertakten*.)

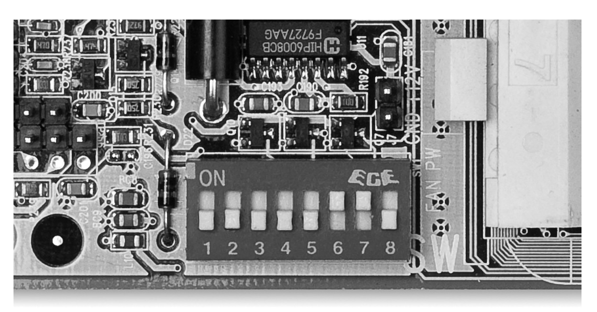


Abb. 3.23: DIP-Schalter auf einem Mainboard

64-Bit-Architektur

Bei der Entwicklung immer neuer Generationen von Mikroprozessoren haben die Ingenieure auch viele physische Aspekte der CPUs erweitert. So wuchs die Breite des externen Datenbusses allmählich von 8 über 16 und 32 bis auf 64 Bit an. Ebenso wuchs die Breite des Adressbusses von 20 über 24 auf 32 (wo sie ein Jahrzehnt verblieb) Bit an.

Auch die technologischen Merkmale änderten sich. Es wurden beispielsweise neue und verbesserte Register hinzugefügt, die schicke Namen wie MMX (*Multimedia Extension*) oder SSE (*Streaming SIMD Extension*) trugen. Eine sehr viel bedeutendere Umwälzung ist seit einigen Jahren im Gange: die Entwicklung hin zur 64-Bit-Architektur.

Die meisten modernen CPUs unterstützen 64-Bit-Verarbeitung. Das bedeutet, dass auf ihnen kompatible 64-Bit-Betriebssysteme wie Windows 8.1 und 64-Bit-Anwendungen ausgeführt werden können. Außerdem werden 32-Bit-Verarbeitung und 32-Bit-Anwendungen bei 32-Bit-Betriebssystemen unterstützt, z.B. bei einigen Linux-Distributionen. Die Mehrzweckregister haben ebenfalls den Sprung auf die 64-Bit-Architektur hinter sich. Der entscheidende Vorteil der 64-Bit-Architektur ist es, dass moderne Systeme erheblich mehr als die 4 Gigabyte RAM unterstützen, auf die 32-Bit-Systeme beschränkt sind.

Mit einem 64 Bit breiten Adressbus kann die CPU 2^{64} Byte Arbeitsspeicher adressieren. Das sind genauer ausgedrückt 18.446.744.073.709.551.616 Byte RAM – eine erkleckliche Menge RAM! Diese Zahl ist derart groß, dass Gigabyte und Terabyte keine geeigneten Einheiten mehr sind, wir verwenden daher Exabyte (2^{60} Byte) oder abgekürzt EB. Mit einem 64-Bit-Adressbus lassen sich 16 Exabyte RAM adressieren.

In der Praxis verbessert die 64-Bit-Architektur die Geschwindigkeit von Programmen, die mit sehr großen Dateien arbeiten, wie etwa Anwendungen zur Videobearbeitung, erheblich. Sie werden bei dieser Art Software eine deutliche Geschwindigkeitssteigerung bemerken, wenn Sie von einem System mit 4 GB RAM auf eines mit 8 oder 16 GB RAM wechseln.

x86 Ältere CPUs können als x86-CPUs zusammengefasst werden, da sie einen Befehlssatz verwenden, der auf der ersten Prozessorarchitektur von Intel beruht. So kann beispielsweise der Intel Core 2 Duo Programme ausführen, die für einen betagten 80386-Prozessor geschrieben wurden, ein Prozessormodell, das in den frühen 1990er-Jahren aktuell war.

x64 Als 64-Bit-Prozessoren allmählich zum Standard wurden, suchten die Marketingleute nach einer Möglichkeit, Programme, Betriebssysteme usw. irgendwie zu kennzeichnen, sodass die Konsumenten auf einen Blick erkennen konnten, ob etwas mit ihren Systemen kompatibel ist oder nicht. Das ist nicht unwichtig, denn geöffnete Software kann im Allgemeinen nicht zurückgegeben werden. Die Marketingexperten entschieden sich für die Bezeichnung x64 und verursachten damit ein ziemliches Durcheinander.

x86-64 Die älteren Sachen für 32-Bit-Systeme wurden mit x86 gekennzeichnet, nicht mit x32, sodass es nun die Kennzeichnungen x86 (alte 32-Bit-Sachen) und x64 (neue 64-Bit-Sachen) gibt. Keine ideale Lösung, aber das Prinzip haben Sie doch erkannt? Um die Verwirrung zu vervollkommnen: x64-Prozessoren können x86-Code ausführen und sind per definitionem ebenfalls x86-Prozessoren! Es ist daher üblich, die beiden Bezeichnungen zu verschmelzen und aktuelle 64-Bit-CPUs als x86-64-Prozessoren zu bezeichnen.

Unterstützung für Virtualisierung

Sowohl Intel als auch AMD haben Unterstützung für das gleichzeitige Ausführen von mehr als einem Betriebssystem in ihre Prozessoren eingebaut. Dieser Vorgang wird als *Virtualisierung* bezeichnet. Virtualisierung ist eine feine Sache und ihr ist ein eigenes Kapitel gewidmet (Kapitel 22), daher erspare ich Ihnen hier die Details. Aus Sicht der CPU ist entscheidend, dass die Virtualisierung früher vollständig durch Software realisiert wurde. Es musste eine Unmenge Code geschrieben werden, damit eine CPU, die für ein einziges Betriebssystem ausgelegt ist, mehrere Betriebssysteme gleichzeitig ausführen konnte. Denken Sie einen Moment darüber nach, was alles damit verbunden ist. Beispielsweise wie Arbeitsspeicher reserviert wird oder welches Betriebssystem gemeint ist, wenn der Benutzer etwas eingibt oder auf ein Symbol klickt. Die Unterstützung der Virtualisierung durch die Hardware hat die Programmierer in hohem Maße entlastet und die Virtualisierung insgesamt erheblich vereinfacht.

Parallelverarbeitung

Moderne CPUs können mehrere Befehle und Befehlsteile gleichzeitig ausführen. Dies nennt man *Parallelverarbeitung*. Ältere Prozessoren mussten hingegen alle Befehle in strikt linearer Weise abarbeiten. Die CPUs erreichen diese Simultanität durch mehrere Pipelines (siehe nächster Absatz), eigenen Cache-Speicher und die Fähigkeit, verschiedene Threads oder Programme gleichzeitig verwenden zu können. Um diese enorme Steigerung der Effizienz durch Parallelverarbeitung wirklich verstehen zu können, sind Kenntnisse der unterschiedlichen Ausführungsstufen erforderlich.

Pipelines Erinnern Sie sich noch an die Vorstellung, eine Kurbel mehrfach zu drehen, um ein Ergebnis von der CPU zu erhalten? Hauptsächlich liegt dies daran, dass die CPU mindestens vier *Ausführungsstufen* bzw. *Phasen* durchlaufen muss, um einen Befehl vom externen Datenbus zu übernehmen, die Berechnung auszuführen und das Ergebnis wieder auf dem externen Datenbus abzulegen:

1. **Fetch**: Daten vom externen Datenbus übernehmen.
2. **Decode**: Ermitteln, welcher Befehl ausgeführt werden soll.
3. **Execute**: Die Berechnung(en) durchführen.
4. **Write**: Die Daten wieder auf dem externen Datenbus ablegen.

Intelligente, getrennt voneinander arbeitende Schaltkreise innerhalb der CPU kümmern sich um die einzelnen Phasen. Wenn ein Befehl auf dem externen Datenbus abgelegt wurde, dann mussten bei den alten Prozessoren die einzelnen Phasen ihre Aufgabe erst einmal abschließen und das Ergebnis der CPU mitteilen, bevor die nächste Phase in Angriff genommen werden konnte, sodass zur Verarbeitung eines Befehls immer mindestens vier Taktzyklen benötigt wurden. Bei jedem Taktzyklus blieben drei der vier Ausführungsstufen untätig. Heute arbeiten die Schaltkreise wie ein Förderband und man spricht von einer *Pipeline*. Durch das Pipelining kann jede Phase in jedem Taktzyklus eine Aufgabe erledigen, was viel effizienter ist. Da es in der CPU mehrere Schaltkreise gibt, die mehrere Aufgaben parallel erledigen können, erweitern wir die Analogie unseres Schachtelmanns um das Pipelining. Dadurch haben wir es nun mit mehreren Schachtel*männern* am Fließband zu tun (Abbildung 3.24)!

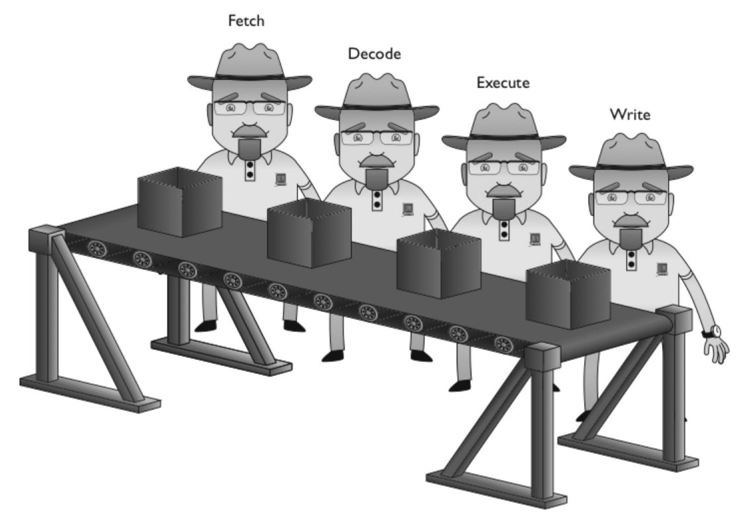


Abb. 3.24: Pipelining

Pipelines sorgen dafür, dass alle Prozessorphasen in einem Takt beschäftigt sind, sodass der Prozessor auch ohne Erhöhung der Taktfrequenz effizienter arbeiten kann. Beachten Sie, dass die CPU vier Phasen besitzt (Fetch, Decode, Execute und Write) und wir daher eine vierstufige Pipeline haben. Keine je hergestellte CPU hatte weniger als vier Ausführungsstufen, und mit den Fortschritten beim Zwischenspeichern der Daten (siehe *CPU-Cache* im nächsten Abschnitt) stieg deren Anzahl im Laufe der Jahre immer weiter an. Aktuelle CPU-Pipelines enthalten in einigen Fällen bis zu 20 Ausführungsstufen.

Das Pipelining ist nicht perfekt. Zuweilen hat es eine Ausführungsstufe mit einem komplexen Befehl zu tun, dessen Abarbeitung mehr als einen Taktzyklus benötigt, sodass die Pipeline gezwungenermaßen angehalten wird. Diese Stopps, auch als *Pipeline-Stalls* bezeichnet, versucht die CPU möglichst zu vermeiden. Tendenziell verursacht die Decode-Phase die meisten Pipeline-Stalls – bestimmte Befehle sind zu komplex und deshalb schwieriger zu decodieren als andere. Aktuelle Prozessoren verwenden daher mehrere Decode-Phasen, um Pipeline-Stalls aufgrund komplexer Decodierung weniger wahrscheinlich zu machen.

Prozessoren bestehen aus mehreren Schaltkreisen, die für verschiedene Berechnungen im PC zuständig sind. Ein Teil beispielsweise, die *ALU* (*Arithmetic Logic Unit*, auch *Integer-Einheit*), führt ganzzahlige Berechnungen ohne Fließkomma durch. $2 + 3 = 5$ ist ein wunderbares Beispiel für eine Integer-Berechnung. Die typische CPU verbringt den größten Teil ihrer Arbeitszeit mit ganzzahligen Berechnungen. Es gibt aber auch spezielle Schaltkreise zur Verarbeitung komplexerer Zahlen, die sogenannte *FPU* (Floating Point Unit, Fließkommaeinheit). Mit einer einzigen Pipeline arbeiteten in jeder Ausführungsstufe nur die Integer-Einheit oder die Fließkommaeinheit. Noch schlimmer war, dass Fließkommaberechnungen häufig sehr, sehr viele Taktzyklen benötigten, wodurch die CPU die Pipe-

line anhalten musste, bis die Fließkommaeinheit die Ausführung des komplexen Befehls abgeschlossen hatte (Abbildung 3.25). Aktuelle CPUs bieten daher mehrere Pipelines, um die Verarbeitung stets in Gang zu halten (Abbildung 3.26).

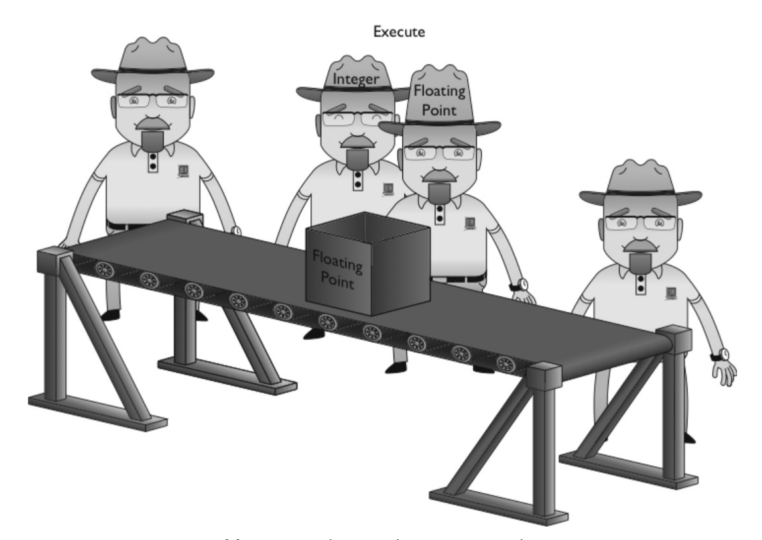


Abb. 3.25: Gelangweilte Integer-Einheit

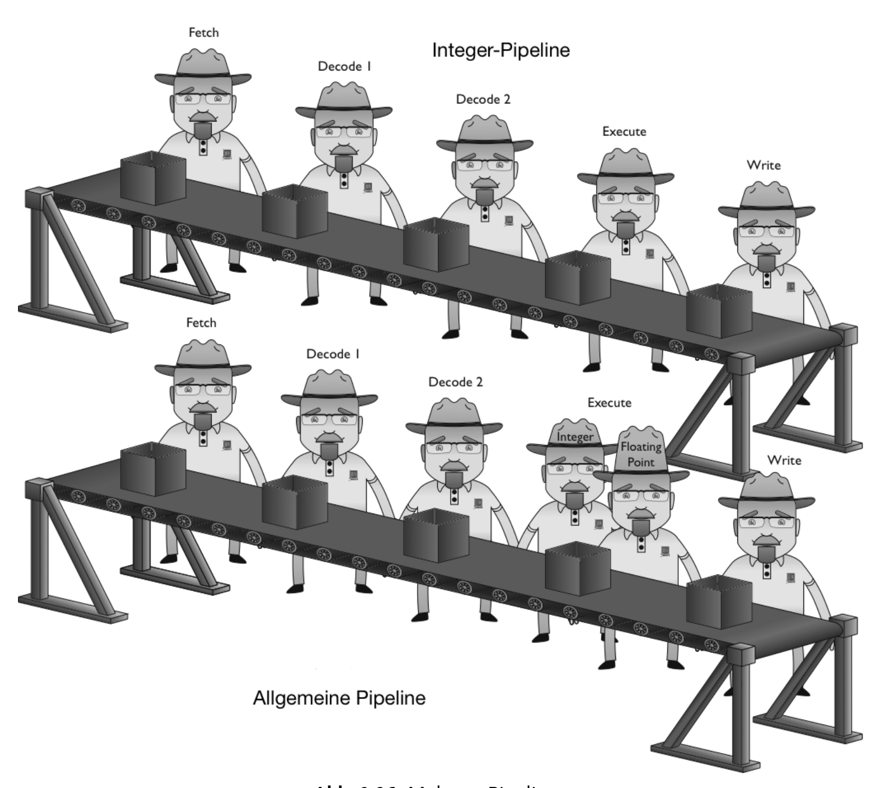


Abb. 3.26: Mehrere Pipelines

CPU-Cache Wenn ein Programm, wie z.B. ein Webbrowser, gestartet und dessen Code zur CPU übertragen wird, dann werden eigentlich viele kleine Programme gleichzeitig ausgeführt. Sobald Sie das entsprechende Symbol doppelklicken, beginnt Windows mit der Übertragung zahlreicher unterschiedlicher Programme zur CPU. Jedes dieser Programme kann in Daten und mehrere kleine Stücke zerlegt werden, die sogenannten *Threads*. Die einzelnen Threads bestehen aus einer Reihe von Befehlen, die auf bestimmte Weise die Daten manipulieren.

Moderne Prozessoren arbeiten die Befehle nicht sequenziell, einen nach dem anderen ab. Es wird nicht erst Schritt 1, dann Schritt 2 usw. abgearbeitet, vielmehr werden die Befehle geeignet umarrangiert. In den meisten Anwendungen werden bestimmte Befehle und Daten häufiger und manchmal immer wieder benötigt und verwendet.

Pipelining-CPUs funktionieren großartig, solange die Pipelines mit Befehlen gefüllt sind. Weil die CPU vom vergleichsweise langsamen Arbeitsspeicher nicht ununterbrochen mit Code versorgt werden kann, kommt es immer wieder einmal zu Pipeline-Stalls bzw. zu sogenannten *Wartezyklen* (*Waitstates*). Um die Anzahl der Waitstates zu verringern, sind die Prozessoren intern mit zusätzlichem, extrem schnellem Speicher ausgestattet, sogenanntem *statischem RAM* (SRAM). In das SRAM werden vorab möglichst viele Befehle geladen, und es enthält Kopien bereits ausgeführter Instruktionen, die möglicherweise vom Prozessor erneut ausgeführt werden müssen (siehe Abbildung 3.27). Das auf diese Weise genutzte SRAM wird *Cache* genannt.

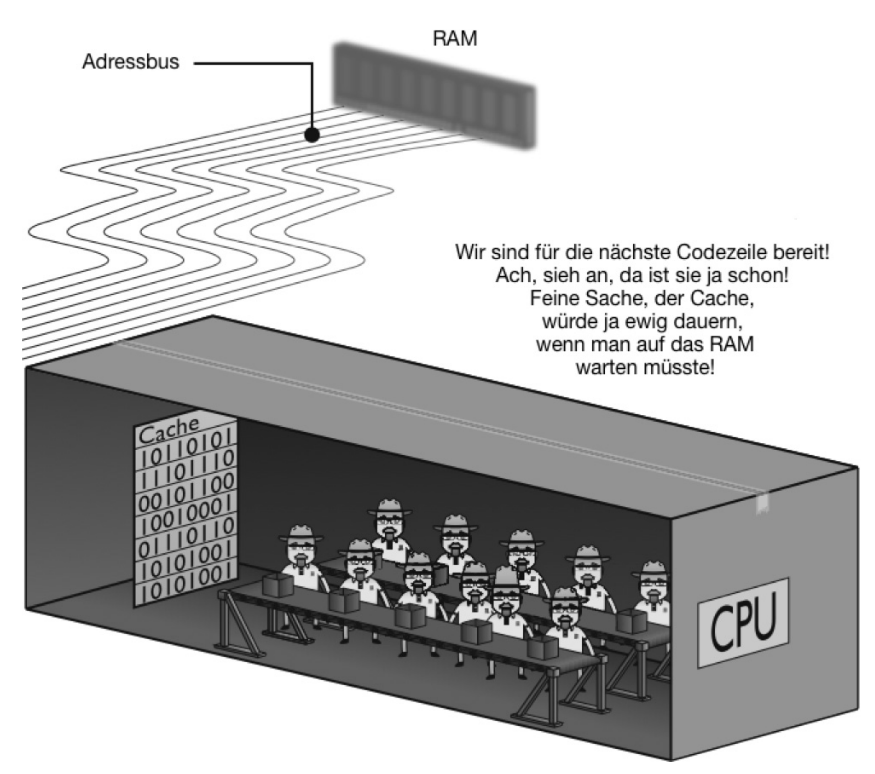


Abb. 3.27: SRAM-Cache

Der SRAM-Cache im Prozessor war zwar winzig und nur etwa 16 KB groß, steigerte die Leistung aber außerordentlich. Er war sogar derart nützlich, dass viele Mainboard-Hersteller dazu übergingen, wei-

teren Cache-Speicher direkt auf den Mainboards hinzuzufügen. Diese Caches waren mit meist 128 bis 512 KB viel größer. Wenn die CPU nach einer Codezeile suchte, sah sie zuerst in ihrem internen Cache nach. Befand sich der Code nicht dort, ging die Suche im Cache auf dem Mainboard weiter. Der Prozessor-Cache wurde *L1-Cache* genannt, weil die CPU hier zuerst nachsah. Der Cache auf dem Mainboard wurde *L2-Cache* genannt, letztlich nicht deshalb, weil er sich auf dem Mainboard befand, sondern weil es sich um den zweiten Cache handelte, in dem die CPU nachsah.

Später trieben Entwickler das Cache-Konzept weiter voran und integrierten auch den L2-Cache in die CPU. Einige CPUs nutzten sogar drei Cache-Ebenen: L1, L2 und L3 (Abbildung 3.28).

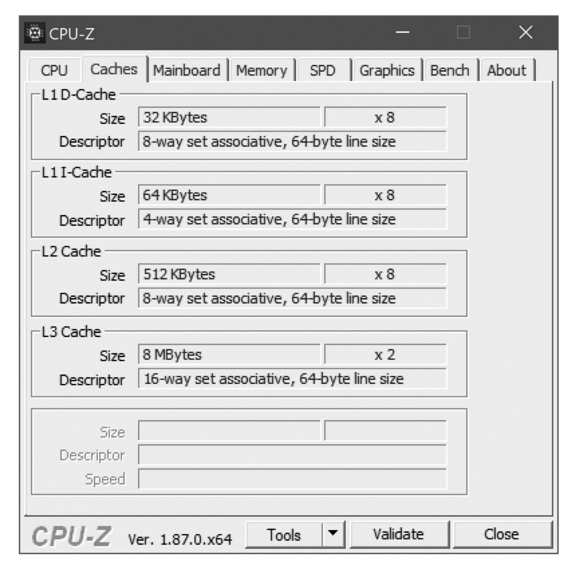


Abb. 3.28: CPU-Z zeigt Informationen über den Cache eines Ryzen-7-Prozessors an.

Bei den ersten Prozessoren, die L2-Cache mitbrachten, war dieser mit im CPU-Gehäuse untergebracht, arbeitete jedoch mit geringerer Taktfrequenz als der L1-Cache. Der L1-Cache war Teil der CPU und wurde ebenso schnell getaktet, der L2-Cache hingegen war physisch von der CPU getrennt und wurde mit halber CPU-Taktfrequenz betrieben.

Durch die Integration des L2-Caches in den Chip entstanden einige neue Begriffe, die die Verbindungen zwischen CPU, MCC, RAM und L2-Cache beschreiben sollten. Der Adressbus und der externe Datenbus (der CPU, MCC und RAM verband) wurden unter der Bezeichnung *Frontside-Bus* zusammengefasst, während die Verbindung zwischen CPU und L2-Cache *Backside-Bus* genannt wurde (siehe Abbildung 3.29). (Auf heutige Computer sind diese Begriffe nur schlecht anwendbar. Sie sind daher nicht mehr gebräuchlich. Siehe dazu den Abschnitt *Integrierter Memory Controller* später in diesem Kapitel.)

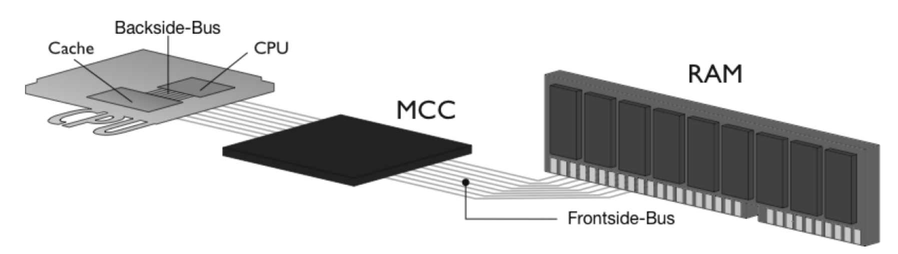


Abb. 3.29: Frontside-Bus und Backside-Bus

Hinweis

Die Mainboard-Hersteller verdoppelten oder vervierfachten sogar den Datendurchsatz des Frontside-Busses, um mit den immer schnelleren Prozessoren Schritt zu halten. Das wird gelegentlich als »double-pumped« bzw. »quad-pumped« bezeichnet.

Wichtig

In der CompTIA A+-Zertifizierungsprüfung wird von Ihnen typischerweise erwartet, dass Sie wissen, dass es sich beim L1-Cache um den kleinsten und schnellsten Cache handelt, der L2-Cache größer und langsamer als der L1-Cache ist, während L3-Cache am größten und langsamsten ist. (Das ist heutzutage nicht mehr ganz richtig, weil L1- und L2-Cache in vielen CPUs gleich schnell arbeiten, in der Prüfung bleibt es jedoch vorläufig dabei.)

Multithreading Als sich die 32-Bit-Architektur auf ihrem Höhepunkt befand, stellte Intel mit dem Pentium 4 einen Prozessor vor, mit dem die Parallelverarbeitung durch *Hyperthreading* einen weiteren Schritt vorangebracht wurde. Diese Technologie ermöglicht es dem Pentium 4, mehrere Threads gleichzeitig auszuführen und wird allgemein als *simultanes Multithreading* bezeichnet. Hyperthreading macht sozusagen aus einer CPU auf dem Chip zwei! Dabei gibt es jedoch einen kleinen Haken.

Abbildung 3.30 zeigt den Task-Manager eines betagten Windows-XP-Systems mit einem Hyperthreading-fähigen Pentium 4. Beachten Sie, dass der CPU-Bereich zweigeteilt ist – Windows »denkt«, es handelt sich um zwei Prozessoren.

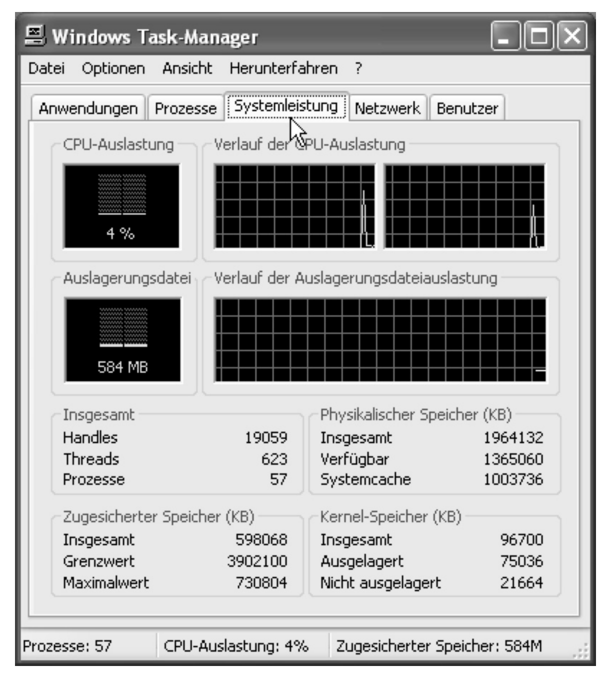


Abb. 3.30: Die Registerkarte SYSTEMLEISTUNG im Task-Manager mit Hyperthreading-fähigem Pentium 4

Multithreading verbessert die Effizienz der CPU, bringt jedoch auch einige Einschränkungen mit sich. Zum einen müssen sowohl Betriebssystem als auch Programme dafür ausgelegt sein, diese Funktion zu verwenden. Zum anderen wird zwar ein zweiter Prozessor simuliert, allerdings verdoppelt sich

dadurch die Rechenleistung nicht, denn die übrigen Ressourcen des Computers bleiben schließlich unverändert.

Tipp

Dies ist der richtige Zeitpunkt, um sich die Übung zu Kapitel 3 anzusehen und zu erfahren, wo Sie CPU-Z herunterladen können und wie Sie es benutzen. Besuchen Sie `http://totalsem.com/100x` und sehen Sie sich »What is CPU-Z« an!

Mehrkernprozessoren

CPU-Taktfrequenzen erreichten zwischen 2002 und 2003 in der Praxis eine Grenze von etwa 4 GHz, was die CPU-Hersteller motivierte, nach neuen Wegen zu mehr Rechnerleistung zu suchen. Obwohl Intel und AMD unterschiedliche Ansichten bei 64-Bit-CPUs vertraten, entschlossen sich doch beide fast zur selben Zeit, zwei CPUs (oder Kerne) auf einem einzigen Chip zu kombinieren und die *Dual-Core-Architektur* zu verwirklichen. Bei Doppelkern-CPUs gibt es nicht nur zwei Prozessorkerne im selben Chip. Eine Dual-Core-CPU besitzt zwei Ausführungseinheiten, aber diese beiden Pipeline-Sätze verwenden gemeinsame Caches und gemeinsames RAM.

Heutzutage sind Mehrkernprozessoren (mit vier, sechs oder acht Kernen) üblich. Spitzenmodelle besitzen sogar 32 Kerne! Bei jeder neuen Generation von Mehrkernprozessoren haben Intel und AMD herumexperimentiert, wie die verschiedenen Cache-Speicher am besten auf die einzelnen Kerne verteilt werden. Abbildung 3.31 zeigt ein weiteres Bildschirmfoto von CPU-Z, hier mit der Aufteilung des Cache-Speichers bei einem Core i7.

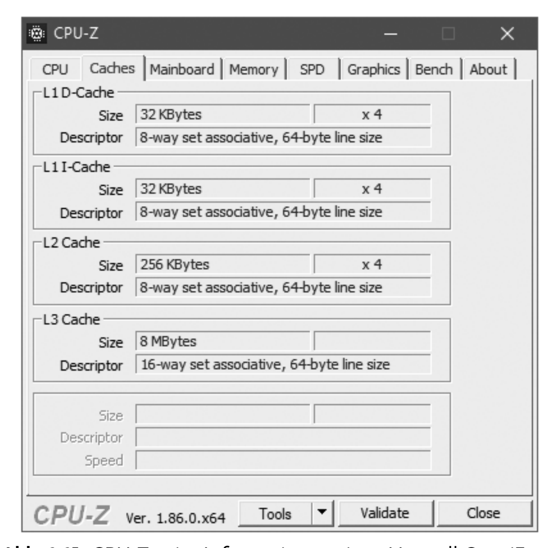


Abb. 3.31: CPU-Z zeigt Informationen eines Haswell Core i7 an.

Sie können Abbildung 3.31 genaue Einzelheiten darüber entnehmen, wie diese Intel-CPU den Cache verwendet. Der Core i7 besitzt L1-, L2- und L3-Cache-Speicher mit einer Größe von 32 KB, 256 KB bzw. 8 MB. (Der L1-Cache ist unterteilt in 32 KB für Daten – der D-Cache – und weitere 32 KB für Befehle (*Instructions*) – der I-Cache.) Jeder Kern verfügt über eigenen L1- und L2-Cache-Speicher. (Das lässt sich anhand des »×4« in der Auflistung der Speichergrößen feststellen.) Den riesigen L3-Cache nutzen alle vier Prozessorkerne gemeinsam. Dieser Speicher ermöglicht es den einzelnen Kernen, miteinander zu kommunizieren und zu kooperieren, ohne häufiger auf den sehr viel langsameren normalen Arbeitsspeicher des Systems zugreifen zu müssen.

Die Hersteller haben die Mehrkern-CPUs dafür ausgelegt, die Rechenlast unabhängig vom Betriebssystem aufzuteilen, was als *Mehrkern-Verarbeitung* bezeichnet wird. Hier ist vom Hyperthreading zu unterscheiden, bei dem Betriebssystem und Programme speziell angepasst werden müssen, um mehrere Threads verwenden zu können. Beachten Sie jedoch, dass selbst bei Mehrkernprozessoren eine Anpassung oder Optimierung der Anwendungen erforderlich ist, um eine wirklich spürbare Auswirkung der Parallelverarbeitung auf die Geschwindigkeit zu erzielen.

Da ein technologischer Fortschritt nicht ausreicht, stellen sowohl Intel als auch AMD Mehrkernprozessoren her, die auch Hyperthreading verwenden. Der Intel Core i9-7960X beispielsweise bietet 16 Kerne, Hyperthreading, 16 MB L2-Cache, 22 MB L3-Cache und Turbo Boost, um das System bei Bedarf mit mehr als 4 GHz zu takten. Das ist schon beeindruckend!

Integrierter Memory Controller

Sämtliche aktuellen Mikroprozessoren besitzen einen *IMC* (*Integrated Memory Controller*), der vom Mainboard in die CPU gewandert ist, um den ein- und ausgehenden Informationsfluss der CPU zu optimieren. Der IMC gestattet eine schnellere Steuerung bestimmter Vorgänge, wie etwa die gemeinsame Nutzung des großen L3-Cache-Speichers durch mehrere Kerne.

Ebenso wie in vielen anderen Bereichen im Computerwesen haben die Hersteller eine Vielzahl unterschiedlicher Varianten des IMCs in ihren Prozessoren verbaut. Das bedeutet in der Praxis, dass verschiedene CPUs auch verschiedene RAM-Typen und voneinander abweichende Speichergrößen verwenden. Die Details der diversen RAM-Varianten hebe ich mir für Kapitel 4 auf. Fürs Erste genügt es, Ihrer Prüfliste für die CPU-Kaufempfehlung den Punkt »Unterstützung verschiedener RAM-Typen« hinzuzufügen.

Integrierte GPU

Wie Sie ausführlich in Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*, nachlesen können, verfügt derjenige Teil des Computers, der für die Bildschirmausgabe zuständig ist, üblicherweise über einen eigenständigen Prozessor, der sich sowohl von der Funktion her als auch von der Architektur von den CPUs unterscheidet, die für übliche Computerarbeiten verwendet werden. Die allgemeine Bezeichnung für diese CPUs lautet *GPU* (*Graphics Processing Unit*, Grafikprozessor). Bis Kapitel 17 erspare ich Ihnen die Einzelheiten, aber es hat sich herausgestellt, dass Grafikprozessoren bestimmte Aufgaben sehr viel effizienter als normale CPUs erledigen können. Die Integration einer GPU in die CPU erhöht die Geschwindigkeit des Computers insgesamt und vermindert dabei gleichzeitig den Energieverbrauch, die Größe und die Kosten. Bei der zunehmenden Verbreitung mobiler Geräte und tragbarer Computer sind diese Vorteile natürlich von großem Wert.

CPUs mit integrierter GPU haben beide der großen Prozessorhersteller herausgebracht. Viele Jahre lang fiel die Entscheidung zwischen den beiden nicht schwer, wenn es darum ging, grafisch anspruchsvolle Programme wie Spiele auszuführen.

Die in vielen Core i3/i5/i7-Prozessoren integrierten *Intel HD Graphics* und *Intel Iris Pro Graphics* sehen im Vergleich mit AMDs *APU* (*Accelerated Processing Unit*,, wie z.B. die AMD A10 ziemlich alt aus. AMD hat schon vor Jahren einen der auf Grafikkarten spezialisierten Hersteller (ATI) übernommen und dessen Technologie zum Bau von Mikroprozessoren mit integrierter CPU und GPU eingesetzt. (Die Spielkonsolen Xbox One und Playstation4 verwenden beispielsweise AMD-APUs.) Intel holt hier aber allmählich auf.

Sicherheit

Alle modernen Prozessoren verfügen über die NX-Bit-Technologie, die es der CPU ermöglicht, bestimmte Speicherbereiche zu schützen. Zusammen mit der Implementierung durch das Betriebssystem können damit bösartige Angriffe auf für den Betrieb des Systems wichtige Dateien verhindert werden. Microsoft bezeichnet dieses Feature als *Datenausführungsverhinderung* (*DEP, Data Execution Prevention*). Seit Windows XP ist es in allen Betriebssystemversionen standardmäßig aktiv (Abbildung 3.32).

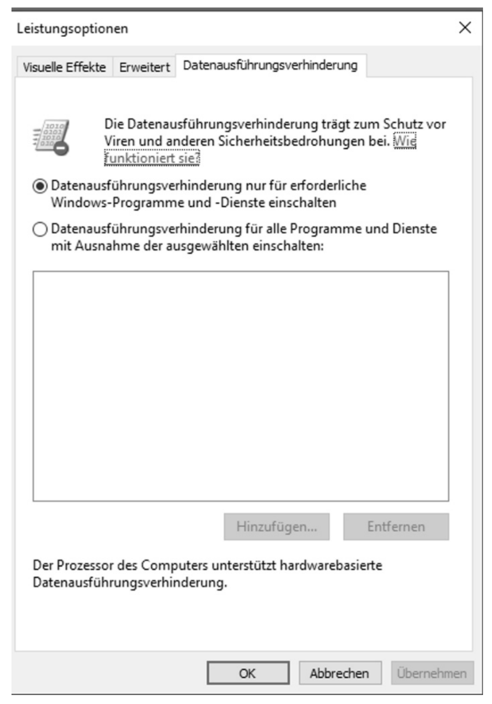


Abb. 3.32: DEP in Windows 10

Das Dumme daran ist nur, dass alle Beteiligten eine andere Bezeichnung für die NX-Bit-Technologie verwenden:

- **Intel**: XD-Bit (e**X**ecute **D**isable, Ausführung deaktiviert)
- **AMD**: Enhanced Virus Protection (verbesserter Virenschutz)
- **ARM**: XN (e**X**ecute **N**ever, niemals ausführen)

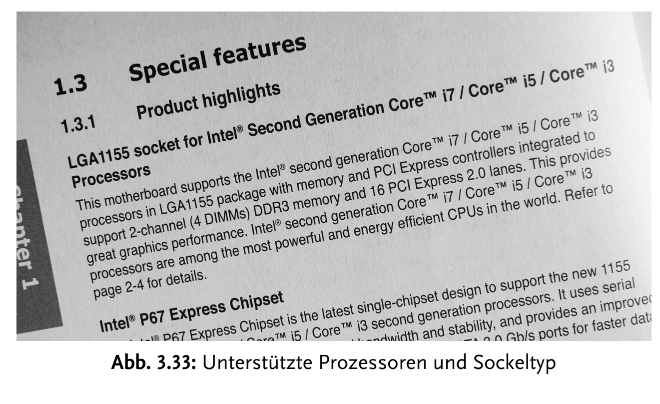
3.4 Installieren von Prozessoren

Nun ist Ihnen die grundlegende Funktionsweise von Prozessoren bekannt und es ist an der Zeit für etwas Praxis. In diesem Abschnitt werden die Auswahl einer geeigneten CPU, die Installation verschiedener Prozessortypen und die Behebung der wenigen Probleme erläutert, denen Sie als Techniker im Umgang mit CPUs begegnen werden.

3.4.1 Auswahl des Prozessors

Bei der Auswahl einer CPU müssen Sie sicherstellen, dass diese zu Ihrem Mainboard passt. Falls Sie ein Mainboard inklusive CPU kaufen, müssen Sie darauf achten, dass Sie eine für Ihre Zwecke geeignete CPU aussuchen. In Kapitel 11 werden die möglichen Einsatzgebiete beschrieben, was Ihnen dabei helfen soll, für jedes davon die passenden Komponenten auszuwählen. Um das große Ganze zu überblicken, ist eine Menge Wissen über all die Kleinigkeiten erforderlich, die es bei einem Prozessor zu beachten gibt. Ich warte daher noch etwas, um dann später zu erklären, warum eine bestimmte CPU am geeignetsten ist. Wir nehmen stattdessen an, dass Sie einen neuen Prozessor in ein bereits vorhandenes Mainboard einbauen wollen. Dabei gibt es für die Auswahl einer funktionierenden CPU zwei entscheidende Kriterien. Erstens unterstützt das Mainboard Prozessoren von Intel oder von AMD? Und zweitens, welcher Sockeltyp befindet sich auf dem Mainboard?

Eine Antwort auf diese beiden Fragen finden Sie entweder im Handbuch des Mainboards oder auf den Webseiten des Herstellers. Abbildung 3.33 zeigt das aufgeschlagene Handbuch eines ASUS-Mainboards an der Stelle, wo die unterstützten Prozessoren und die Sockeltypen aufgeführt sind.



1.3 Special features

1.3.1 Product highlights

LGA1155 socket for Intel® Second Generation Core™ i7 / Core™ i5 / Core™ i3 Processors

This motherboard supports the Intel® second generation Core™ i7 / Core™ i5 / Core™ i3 processors in LGA1155 package with memory and PCI Express controllers integrated to support 2-channel (4 DIMMs) DDR3 memory and 16 PCI Express 2.0 lanes. This provides great graphics performance. Intel® second generation Core™ i7 / Core™ i5 / Core™ i3 processors are among the most powerful and energy efficient CPUs in the world. Refer to page 2-4 for details.

Intel® P67 Express Chipset

P67 Express Chipset is the latest single-chipset design to support the new 1155 ... i5 / Core™ i3 second generation processors. It uses serial ... bandwidth and stability, and provides an improve...

Abb. 3.33: Unterstützte Prozessoren und Sockeltyp

Ebenso wie Intel und AMD viele verschiedene CPU-Typen herstellen, bauen die Mainboard-Hersteller eine Reihe unterschiedlicher Sockel. Im Laufe der Jahre wurden Hunderte verschiedene Sockel entwickelt. In Tabelle 3.2 sind die wichtigen von Intel bzw. AMD verwendeten Sockeltypen aufgeführt. Die CompTIA hat üblicherweise sowohl Sockelnummer bzw. -name als auch (bei Sockeln von Intel) die alternative Bezeichnung abgefragt. Deshalb habe ich in der Tabelle die neuesten Namen und alternativen Bezeichnungen aufgenommen.

Wichtig

In den CompTIA A+-Lernzielen sind keine Prozessorsockel aufgeführt, in früheren Prüfungen wurden jedoch häufig Fragen dazu gestellt. Hoffentlich bleiben Ihnen solche Fragen erspart, aber es ist sicher keine schlechte Idee, die Sockel zu kennen. Von der Prüfung einmal abgesehen, sollten Sie wissen, dass zu jeder CPU ein bestimmter passender Sockel gehört, um zu gewährleisten, dass das Motherboard eines Kunden den für die empfohlene CPU passenden Sockel besitzt.

Sockel	Alternativer Name	Plattform	CPU
LGA 1150	H3	Intel	Core i3/i5/i7, Pentium, Celeron, Xeon
LGA 1151	H4	Intel	Core i3/i5/i7, Pentium, Celeron, Xeon
LGA 2011	R oder R3	Intel	Core i7, Core i7 Extreme Edition, Xeon
LGA 2066	R4	Intel	Core i5/i7/i9, Xeon
FM2+	-	AMD	A-Reihe
AM3+	-	AMD	FX, Opteron
AM4	-	AMD	Ryzen, A-Reihe
TR4	-	AMD	Ryzen Threadripper

Tabelle 3.2: Gängige Sockel

Entschlüsseln der Prozessorkennung

Intel und AMD verwenden unterschiedliche Nummerierungsmethoden, die Ihnen dabei helfen, verschiedene Prozessoren mit ähnlichen Namen zu vergleichen, wie z.B. Modelle des Core i5. Intel und AMD verwenden ziemlich ähnliche Systeme. Nachfolgend werden beide vorgestellt.

Die Kennung von Intel-Prozessoren folgt einem klaren Muster. Die Prozessorbezeichnung Intel Core i7 7500 U bedeutet beispielsweise:

- Intel Core = Markenname
- i7 = genauere Modellbezeichnung
- 7 = die siebte Generation des Modells
- 500 = Artikelnummer
- U = das sogenannte Alphasuffix (U bedeutet, dass es sich um einen Desktop-Prozessor mit geringem Stromverbrauch handelt)

Vergleichen Sie diesen Prozessor mit dem Modell Intel Core i7 8650 U, bei dem die Kennung Folgendes bedeutet:

- Intel Core = Markenname
- i7 = genauere Modellbezeichnung
- 8 = die achte Generation des Modells
- 650 = Artikelnummer
- U = Alphasuffix (U bedeutet, dass es sich um einen Desktop-Prozessor mit geringem Stromverbrauch handelt)

Und so entschlüsseln Sie die Kennung eines AMD Ryzen 7 2700X:

- AMD = Markenname
- 7 = Marktsegment
- 2 = Generation
- 7 = Leistungsniveau
- 00 = Modellnummer
- X = Leistungssufix (X bedeutet hohe Leistung)

Tipp: Informationen über Prozessoren

Sowohl Intel als auch AMD bieten auf ihren Websites erschöpfende Informationen über ihre neuesten CPUs. Auf den drei hier aufgeführten Websites finden Sie Einzelheiten zum Support und Empfehlungen zum Umgang mit bestimmten Sockeln bei Upgrades.Besuchen Sie die Websites und erkunden Sie die CPUs. Und erstellen Sie ein Lesezeichen in Ihrem Webrowser, um später bei Bedarf wieder darauf zugreifen zu können.

`https://ark.intel.com`

`https://www.amd.com/de/products/processors-desktop`

`https://www.amd.com/de/products/processors-laptop`

3.4.2 Mögliche Probleme bei der Installation

Beim Installieren einer CPU müssen Sie sehr vorsichtig im Umgang mit den winzigen Pins sein. Außerdem müssen Sie sich vergewissern, dass das Netzteil genügend Leistung für den Prozessor und all die anderen Komponenten des Computers bereitstellen kann. Darüber hinaus müssen Sie für eine angemessene Kühlung sorgen. Schließlich können Sie entscheiden, ob Sie es bei den Werkseinstellungen belassen möchten oder eine Übertaktung der CPU in Angriff nehmen.

Sockeltypen

Achten Sie bei der Installation einer CPU darauf, nicht versehentlich einen der winzigen Pins zu verbiegen. Die genaue Position der Pins unterscheidet sich zwischen Intel und AMD. Bei Mainboards für

Intel-CPUs besitzt der Sockel Hunderte dieser winzigen Pins, die exakt mit den Kontakten auf der Unterseite der CPU ausgerichtet sind (Abbildung 3.34). Intel-CPUs verwenden eine als *LGA* (*Land Grid Array*) bezeichnete Bauform, bei der sich auf der Unterseite des Prozessors Hunderte von Kontaktstellen befinden, die genau zu den Pins auf dem Sockel passen.

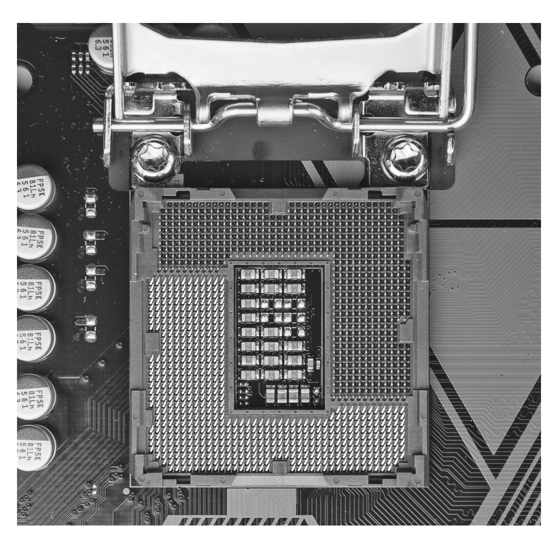


Abb. 3.34: Sockel für Intel-CPUs mit Pins

Beim AMD-CPUs ist es umgekehrt: Der Sockel besitzt die Kontaktstellen (Abbildung 3.35) und die Pins befinden sich auf der Unterseite der CPU. Diese Bauform heißt *PGA* (*Pin Grid Array*).

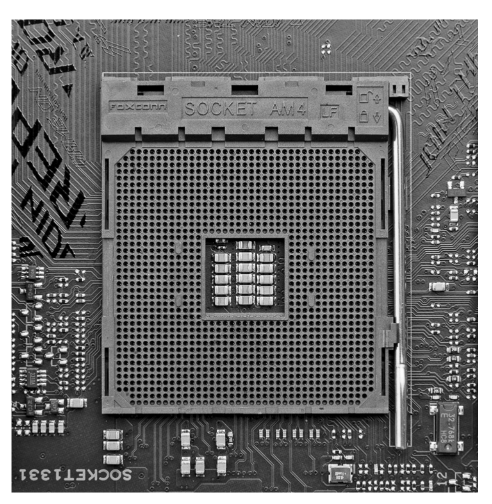


Abb. 3.35: Sockel für AMD-CPUs ohne Pins

Alle Prozessoren und Sockel sind deutlich gekennzeichnet, damit sie nicht versehentlich verkehrt herum eingesetzt werden. Betrachten Sie die Unterseite der CPU auf der linken Seite in Abbildung 3.36. Wie Sie sehen, bilden die Pins *kein* vollständiges Quadrat, da einige fehlen. Nun sehen Sie sich die Oberseite auf der rechten Seite an. Sehen Sie die kleine dreieckige Markierung? Der Sockel besitzt eine entsprechende Markierung, sodass Sie CPU und Sockel korrekt ausrichten können.

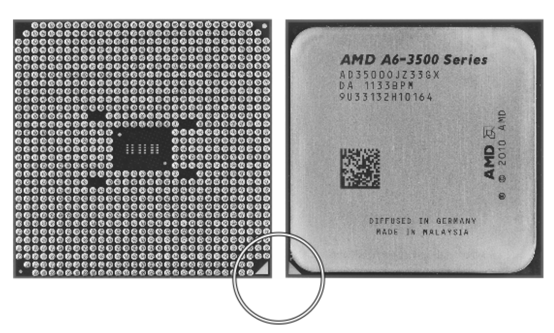


Abb. 3.36: Unter- und Oberseite einer CPU

Bei beiden Sockeltypen findet ein kleiner Hebel Verwendung, den Sie zunächst ein wenig herunterdrücken und dann vom Sockel fortbewegen müssen, um den Haltemechanismus zu lösen (Abbildung 3.37) Danach können Sie den Hebel komplett umlegen und schließlich die Halteklammer entfernen (Abbildung 3.38).

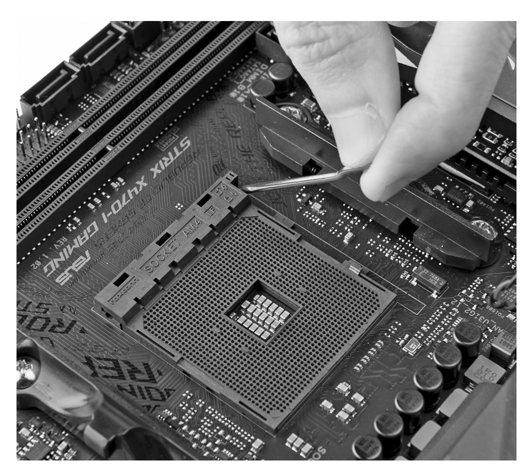


Abb. 3.37: Der Hebel zum Lösen des Haltemechanismus

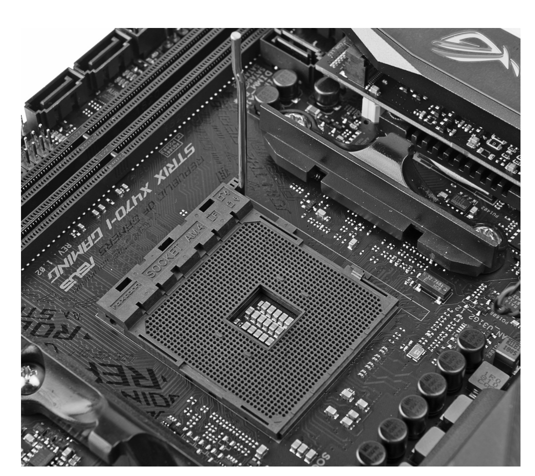


Abb. 3.38: Der geöffnete Sockel

Setzen Sie nun den Prozessor ganz sanft in korrekter Ausrichtung auf den Sockel. Wenn das nicht »flutscht«, sollten Sie die Ausrichtung des Prozessors überprüfen und es erneut versuchen. Die Sockel heißen nicht umsonst *ZIF-Sockel* (oder laut Wikipedia *Nullkraftsockel*, wobei *ZIF* für *Zero Insertion Force* steht) und es darf wirklich keinerlei Kraft erforderlich sein, um die CPU einzusetzen.

Kühlung

Die Leistungsfähigkeit moderner Prozessoren verlangt einen gewissen Tribut: Sie benötigen Energie. Genauer ausgedrückt elektrische Leistung, die in der Einheit *Watt* gemessen wird. (Siehe dazu auch Kapitel 7, *Netzteile*.) Haben Sie schon mal eine Glühbirne berührt, die ein paar Minuten lang eingeschaltet war? Autsch! Ein Prozessor erwärmt sich im Betrieb ebenfalls sehr.

Um leistungsfähigere CPUs herstellen zu können, mussten die Prozessorhersteller die Anzahl der mikroskopisch kleinen Transistorschaltungen in der CPU ständig erhöhen. Je mehr Transistoren eine CPU besitzt, desto mehr Energie ist erforderlich und umso wärmer wird sie. Prozessoren vertragen Hitze nicht besonders gut und moderne CPUs benötigen eine aktive Kühlung, um überhaupt zu funktionieren. Heutzutage verwenden praktisch alle Prozessoren Kühlkörper und Lüfter, um die Wärme abzutransportieren.

Wichtig

Wenn nur ein Kühlkörper für einen Chip vorhanden ist (kein Lüfter), spricht man von *passiver Kühlung*. Eine Kombination aus Kühlkörper und Lüfter bietet eine *aktive Kühlung*.



Abb. 3.39: Intels Kühlkörper/Lüfter-Baugruppe

Ein Kühlkörper aus Kupfer oder einem anderen Metall dient zum Abführen von Wärme. Abbildung 3.39 zeigt den typischen Kühlkörper/Lüfter von Intel-Geräten. Hier sind einige weitere Kühlmethoden:

- **OEM-Lüfter**: Die im Einzelhandel erhältlichen Intel-Prozessoren, die auch Boxed-Version genannt werden, enthalten für gewöhnlich einen passenden OEM-Kühlkörper mit Lüfter. OEM (*Original Equipment Manufacturer*) bedeutet in diesem Fall, dass Intel die Kühlbaugruppe produziert. Für in großen Stückzahlen und nicht in Originalverpackung gekaufte CPUs ist allerdings ebenfalls der Begriff »OEM-CPUs« gebräuchlich. Sie werden normalerweise ohne Lüfter geliefert. Verrückt, oder? Bei den OEM-Lüftern können Sie nämlich absolut sicher sein, dass sich diese auch für den jeweiligen Prozessor eignen.
- **Spezielle Lüfter**: Viele Unternehmen bieten für verschiedene Prozessoren Kühlkörper und Lüfter von Dritttherstellern an. Üblicherweise sind diese den OEM-Lüftern überlegen und können die Wärme besser abführen. Diese Lüfter ziehen durch ihr tolles Aussehen oft unweigerlich die Blicke auf sich. Manche dieser Lüfter sind sogar beleuchtet, sodass sie im System wirklich beeindruckend aussehen (Abbildung 3.40).

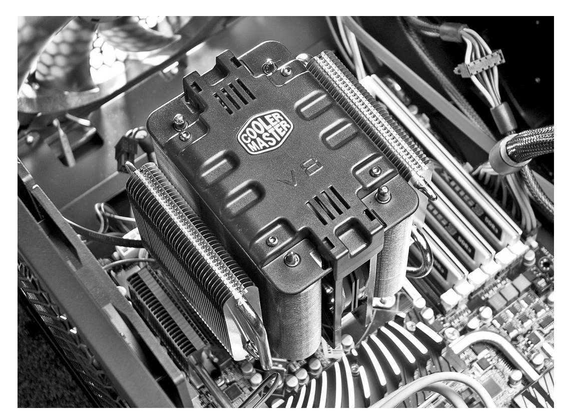


Abb. 3.40: Sieht dieser Lüfter nicht beeindruckend aus?

Die letzte Kühlmethode ist auch die beeindruckendste: *Flüssigkeitskühlung*! Dabei wird eine Flüssigkeit (üblicherweise Wasser) durch einen Metallblock geleitet, der oben auf dem Prozessor aufsitzt und die Wärme absorbiert. Die Flüssigkeit wird vom Metallblock erwärmt, aus dem Block heraus in eine Kühlvorrichtung transportiert und dann wieder durch den Block gepumpt. Alle Flüssigkeitskühlsysteme bestehen also aus drei wesentlichen Komponenten:

- Einem hohlen Metallblock, der auf dem Prozessor aufsitzt
- Einer Umwälzpumpe zum Transport der Flüssigkeit
- Einer Vorrichtung zum Kühlen der Flüssigkeit

Dazu kommen natürlich noch etliche Schläuche, um die Komponenten miteinander zu verbinden. Abbildung 3.41 zeigt einen typischen flüssig gekühlten Prozessor.



Abb. 3.41: Ein flüssig gekühlter Prozessor

Eine Reihe von Unternehmen vertreiben diese Flüssigkeitskühlsysteme. Zwar sehen diese Vorrichtungen wahrlich beeindruckend aus und können den Prozessor auch wirklich kühlen, aber wenn Sie den Rechner nicht übertakten oder großen Wert auf ein möglichst lautloses System legen, dann sollte ein guter Lüfter mit Kühlkörper mehr als ausreichen.

Wichtig

In manchen Fällen kann man ein System ohne CPU-Lüfter einrichten, was dann als lüfterlose oder passive Kühlung bezeichnet wird. Sieht man einmal von mobilen Geräten (wie Apples iPad) ab, die keine Lüfter besitzen, kann dieser Begriff ziemlich irreführend sein. Beispielsweise besitzen die Xeon-CPUs in den Ser-

vern in meinem Büro nur Kühlkörper ohne Lüfter. Allerdings sind sie über Rohrleitungen direkt mit den Gehäuselüftern verbunden und fungieren so als aktive CPU-Kühlung. Darauf muss man erst mal kommen!

Lesen Sie hierzu auch den Abschnitt *Jenseits von A+* am Ende dieses Kapitels.

Wenn Sie sich schließlich ein Kühlsystem für Ihren Computer ausgesucht haben, muss es am Mainboard angeschlossen werden. Um die Ausrichtung des Lüfters festzulegen, sollten Sie die Position des Stromanschlusses überprüfen. Achten Sie darauf, dass die drei- oder vieradrige Leitung bequem bis zur Steckerleiste auf dem Mainboard verlegt werden kann (Abbildung 3.42). Drehen Sie den Lüfter in eine andere Position, falls die Länge der Leitung nicht ausreicht. Wenn Sie Schwierigkeiten haben, die Steckerleiste für den Anschluss des Lüfters zu finden, sehen Sie im Handbuch des Mainboards nach.

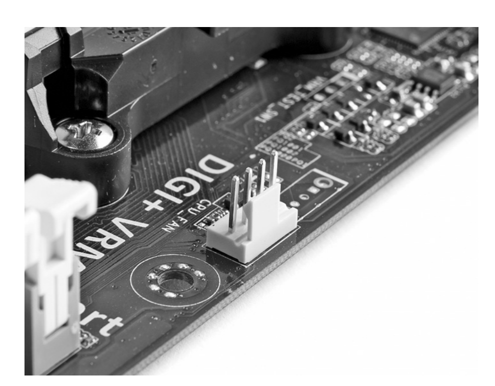


Abb. 3.42: Die Steckerleiste für den Anschluss des Kühlsystems

Bevor Sie den Kühlkörper einbauen, müssen Sie etwas *Wärmeleitpaste* auf die CPU auftragen. Bei vielen Kühlkörpern ist die Wärmeleitpaste bereits aufgetragen, die dann mit einer Art rechteckiger Folie bedeckt ist. Sie müssen die Folie vor der Montage des Kühlkörpers abziehen. Wenn Sie die Wärmeleitpaste aus einer der im Handel erhältlichen kleinen Spritzen auftragen (siehe Abbildung 3.43), sollten Sie beachten, dass nur sehr wenig von dieser Paste benötigt wird! Tragen Sie diese möglichst dünn und gleichmäßig auf der gesamten Oberfläche auf. Anders als bei so vielen anderen Dingen gilt hier: Weniger ist mehr!

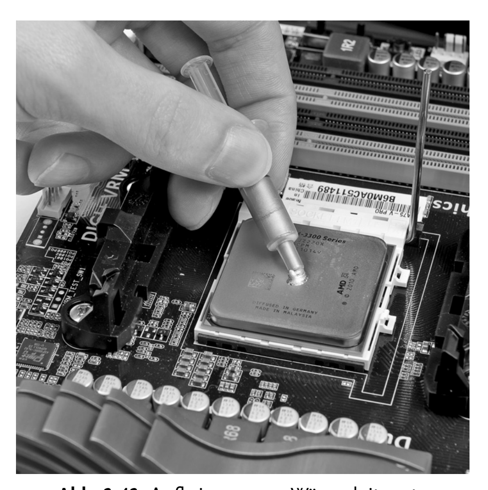


Abb. 3.43: Aufbringen von Wärmeleitpaste

Wie der Lüfter montiert wird, hängt vom Hersteller ab. Die Geräte von Intel besitzen vier Installationsklammern, die nach leichtem Druck mit einem »Klick« in den entsprechenden Öffnungen auf dem Mainboard einrasten. AMD-Lüfter verwenden üblicherweise Metallklammern, die an beiden Seiten des Sockels befestigt werden und eine Art Hebelverschluss (Abbildung 3.44).

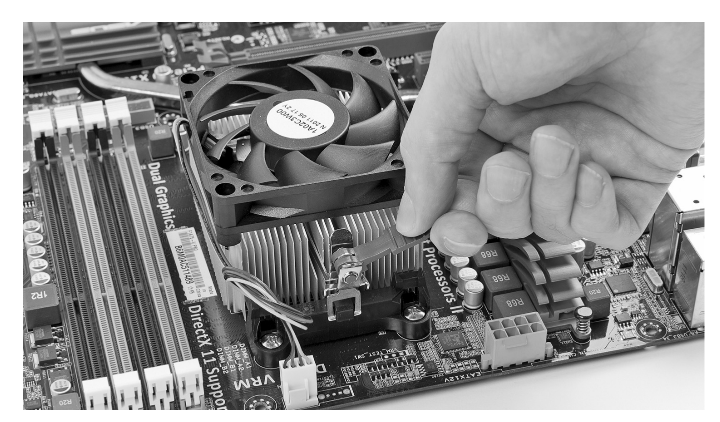
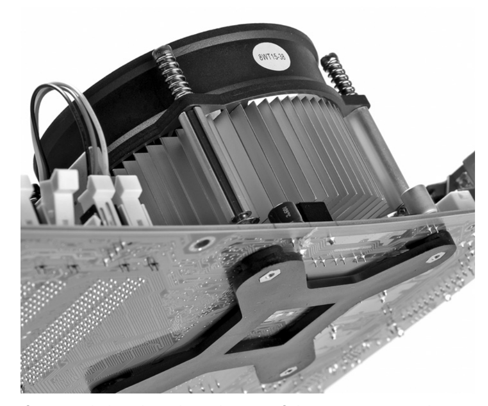


Abb. 3.44: Ein OEM-Lüfter für AMD-Prozessoren

Schließlich gibt es viele Lüfter auf dem Zubehörmarkt, die mit Schrauben auf der Unterseite des Mainboards befestigt werden (Abbildung 3.45). Das heißt, Sie müssen entweder das Mainboard aus dem Gehäuse entfernen oder aber den Lüfter installieren, bevor das Mainboard in das Gehäuse eingesetzt wird.


Abb. 3.45: Dieser Lüfter wird durch Schrauben auf der Unterseite des Mainboards befestigt.

Vergessen Sie den letzten Schritt nicht, nämlich den Lüfter mit dem Stromkabel an die entsprechende Steckerleiste auf dem Mainboard anzuschließen!

Übertakten

Damit die CPU funktioniert, müssen die Mainboard-Geschwindigkeit, der Multiplikator und die Spannung korrekt eingestellt sein. In den meisten modernen Systemen verwendet das Mainboard die CPUID-Funktionen, um diese Einstellungen automatisch vorzunehmen. Bei einigen Mainboards können Sie diese Einstellungen jedoch auch manuell festlegen, indem Sie einen Jumper oder einen DIP-Schalter verwenden, eine CMOS-Einstellung ändern oder auch entsprechende Software einsetzen. Viele Enthusiasten ändern diese Einstellungen bewusst ab, um die Leistung zu erhöhen.

Hinweis

In Kapitel 5 werden das CMOS-Setup-Programm und die Speichermethode für permanente Daten ausführlich erläutert. Allerdings zeigt die Erfahrung, dass wissbegierige Lernende an dieser Stelle unvermeidlich experimentieren wollen, daher vorab einige Informationen. Sie können das CMOS-Setup-Programm verwenden, indem Sie beim Systemstart eine bestimmte Taste gedrückt halten. Dies muss im Textmodus geschehen, lange bevor irgendwelche Meldungen zum Start von Windows angezeigt werden. Bei den meisten Systemen muss `Entf` gedrückt werden, aber schauen Sie im Zweifel auf den Bildschirm, dort wird stets angegeben, welche Taste diesem Zweck dient. Aber Vorsicht! Ändern Sie mit dem CMOS-Setup-Programm keinesfalls irgendetwas, das Sie nicht genau verstehen. Und lesen Sie Kapitel 5!

In den Zeiten der Intel-80486-CPU betrieben die Leute ihre Systeme absichtlich mit einem Takt, der über dem lag, für den die CPU ausgelegt war. Man bezeichnet das als *Übertaktung*, und es funktionierte. Nun, *manchmal* funktionierten die Systeme, mitunter aber auch nicht. Intel und AMD geben für ihre Prozessoren aus gutem Grund bestimmte Taktfrequenzen an, und dabei handelt es sich um die höchste Geschwindigkeit, bei der sie garantiert funktionieren.

Bevor ich fortfahre, muss ich Sie warnen, dass die absichtliche Übertaktung einer CPU unmittelbar die Garantie erlöschen lässt. Durch Übertaktung können CPUs zerstört werden. Die Übertaktung kann Ihr System instabil machen und häufig abstürzen lassen. Ich will die Praxis der Übertaktung weder befürworten noch verurteilen. Mein Ziel ist hier nur, Sie über diese Vorgehensweise zu informieren. Sie müssen Ihre eigene Entscheidung treffen. Wenn ein Kunde eine Übertaktung vornehmen möchte, müssen Sie ihn auf die potenziellen Konsequenzen hinweisen.

Die CPU-Hersteller mögen die Übertaktung nicht. Warum sollten Sie mehr Geld für einen schnelleren Prozessor ausgeben, wenn Sie eine billigere, langsamere CPU nehmen und diese mit einer höheren Geschwindigkeit betreiben können? Intel und AMD mussten sich jedoch dem wachsenden Druck der Enthusiasten beugen und beide Unternehmen bieten Dienstprogramme an, die Ihnen beim Übertakten der jeweiligen CPUs helfen:

- **Intel Extreme Tuning Utility (Intel XTU)**: Hierfür wird ein Performance Tuning Protection Plan angeboten (eine Art Versicherung), den Sie ernsthaft in Betracht ziehen sollten, wenn Sie sich zur Nutzung des Tools entschließen.
- **AMD Overdrive Utility**: Hier gibt es keine weitere Gewährleistung – Sie sind auf sich allein gestellt.

Die meisten Leute nehmen ein paar Anpassungen vor und übertakten ihre Rechner damit erfolgreich. Erstens können Sie über Jumper, CMOS-Einstellungen oder die Software-Konfiguration den Bustakt des Systems erhöhen. Zweitens muss man häufig die an der CPU angelegte Spannung ein wenig erhöhen, um für Stabilität zu sorgen. Dazu ändern Sie einen Jumper oder eine CMOS-Einstellung (Abbildung 3.46).

Durch das Überschreiben der Standardwerte können Sie Ihr System völlig unbrauchbar machen, was so weit gehen kann, dass das Mainboard selbst dann nicht mehr funktioniert, wenn Sie die CPU entfernen und eine neue installieren. (Außerdem besteht ein gewisses Risiko, den Prozessor zu toasten, allerdings enthalten moderne Prozessoren Schaltkreise, die sie rechtzeitig vor dem Überhitzen abschalten.) Bei den meisten Mainboards gibt es einen Jumper, der *CMOS-Clear* oder *CLRTC* genannt wird (Abbildung 3.47), über den wieder die CMOS-Standardeinstellungen gesetzt werden können. Bevor Sie versuchen, ein modernes System zu übertakten, sollten Sie sich darüber informieren, wo sich der CMOS-Clear-Jumper befindet und wie er genutzt wird! Lesen Sie all das am besten im Mainboard-Handbuch nach.

Zum Löschen der CMOS-Einstellungen müssen Sie den PC ausschalten. Nehmen Sie dann eine dieser winzigen Plastik-Steckbrücken (die offiziell *Shunt* genannt werden) und schließen Sie mit ihr den Kontakt zwischen den zwei Anschlüssen. Entfernen Sie dann die Steckbrücke wieder. Anschließend starten Sie den PC und rufen sofort das CMOS-Setup-Programm auf, um dort die erforderlichen Einstellungen wiederherzustellen.

Click BIOS 4 msi F12
X99S SLI PLUS
19:55
Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz
Current CPU Frequency 3.30 GHz (33 x 100.00 MHz)
Current DRAM Frequency 2133 MHz
Memory Size : 16384 MB
Temperature
CPU 36℃
Motherboard 38℃
Version E7885IMS V1.4(140)
Boot device priority
OC GENIE
Motherboard settings
SETTINGS
OC
Use USB to flash/save BIOS
M-FLASH
Overclocking HOT KEY
Voltage Setting
> DigitALL Power
SVID Communication [Auto]
VCCIN Voltage 1.808V Auto
CPU Core/Ring Voltage Mode [Auto]
CPU Core Voltage 0.977V 1.3
CPU Ring Voltage Auto
CPU SA Voltage Mode [Manual Mode]
CPU SA Voltage Auto
CPU VCCIO Voltage 1.056V Auto
DRAM CH_A/B Voltage 1.200V Auto
DRAM CH_C/D Voltage 1.200V Auto
DRAM CH_A/B VPP Voltage 2.512V Auto
DRAM CH_C/D VPP Voltage 2.496V Auto
DRAM CH_A/B VREF Voltage Auto
DRAM CH_C/D VREF Voltage Auto
PCH 1.05 Voltage Auto
PCH 1.5 Voltage Auto
Other Setting
CPU Memory Changed Detect [Enabled]
> CPU Specifications
> MEMORY-Z
> CPU Features
HELP INFO
Addition CPU Voltage
↑↓: Move
→←: Group Jump
Enter: Select
+/-: Value
F1: General Help

Abb. 3.46: Manuelle Änderung der CPU-Einstellungen mit dem CMOS-Setup-Programm

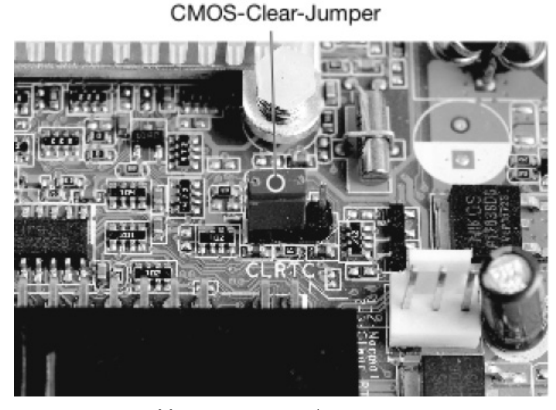


Abb. 3.47: CMOS-Clear-Jumper

3.5 Fehlerbehebung

Bei der Fehlerbehebung von CPUs gibt es zwei Kategorien: Überhitzung und Totalausfall, wobei eine Überhitzung sehr viel häufiger vorkommt als ein Totalausfall. Wenn eine CPU erst einmal ordnungs-

gemäß installiert ist und funktioniert, bereitet sie nur selten Probleme. Die einzige Ausnahme tritt auf, wenn Sie der CPU zu schnell zu viel Leistung abverlangen. Ihr PC wird dann schwerfällig und träge. Der Intel Atom-Prozessor in meinem betagten Netbook beispielsweise leistet gute Dienste beim Surfen im Internet, Schreiben von E-Mails und Verfassen grandioser Kapitel für ihr Lieblingslehrbuch. Aber wenn Sie versuchen, ein anspruchsvolleres Spiel als *Half-Life* (das Original, um 1998 erschienen) zu spielen, gerät der Rechner ins Stottern, meldet Fehler und will einfach nicht mehr mitspielen.

Die meisten CPU-Probleme werden durch fehlerhafte Installation oder ungünstige Umgebungsbedingungen verursacht, die zu einer Überhitzung führen. Ganz selten werden Sie einen Totalausfall erleben, aber wir werden auch auf Hinweise für diesen Fall achtgeben.

3.5.1 Anzeichen für Überhitzung

Fehler bei der Installation einer CPU führen entweder zu gar nichts (das heißt, beim Einschalten des Rechners passiert überhaupt nichts), oder zu einem baldigen Systemabsturz. Dank der ZIF-Sockel können Sie fast mit Sicherheit davon ausgehen, dass das Problem nicht der Prozessor selber ist, sondern eher in einer fehlerhaften Montierung des Kühlkörpers oder des Lüfters zu suchen ist. Es folgt eine kurze Prüfliste möglicher Probleme, die Sie kontrollieren sollten, wenn es Schwierigkeiten bei der Installation des Prozessors gibt:

1. Zu viel Wärmeleitpaste kann den Wärmefluss von der CPU zum Kühlkörper behindern und dazu führen, dass sich die CPU sehr schnell aufheizt. Alle modernen CPUs besitzen jedoch Ausfallsicherungen, die für eine rechtzeitige Abschaltung sorgen, wenn durch die Hitze eine Beschädigung droht.
2. Zu wenig oder ungleichmäßig aufgetragene Wärmeleitpaste kann ebenfalls ein Aufheizen der CPU verursachen und somit konsequenterweise die automatische Abschaltung auslösen.
3. Wenn es übersehen wird, den Lüfter an die Stromversorgung des Mainboards anzuschließen, kann dies zu einer Überhitzung der CPU und deren Abschaltung führen.

Es kann knifflig sein, Fehler bei der Installation des Lüfters oder des Kühlkörpers festzustellen, wenn man ihnen erstmals begegnet. Der Startbildschirm im Textmodus erscheint vielleicht noch, möglicherweise gelangen Sie sogar bis zur Installation von Windows, bevor der Rechner abstürzt. Der entscheidende Punkt ist, dass sich die CPU, sobald sie Arbeit zu bewältigen hat, so stark erhitzt, dass der fehlerhaft verbaute Kühlkörper die Wärme nicht schnell genug abführen kann und die CPU sich abschaltet.

Bei Systemen, die schon länger laufen, können die Umgebungsbedingungen für Probleme ausschlaggebend sein. Der Ausfall der Klimaanlage meines Büros (das im Herzen des sehr heißen Texas gelegen ist) im letzten Sommer sorgte beispielsweise dafür, dass überall im Büro die Rechner nicht mehr ordentlich arbeiteten. Einige fielen sogar vollständig aus. (Das war der richtige Moment, um den Laden zuzumachen und die Leute an den Strand zu schicken, aber das ist eine andere Geschichte.) Am nächsten Tag rief ein Kunde an und beschwerte sich darüber, dass sein Computer sich ständig neu startet und nur langsam arbeitet. Als ich vor Ort war, stellte ich fest, dass in dem Haus sieben Katzen lebten. Das Öffnen des Computers erwies sich als wahrhaftig haarige Angelegenheit: Der Lüfter war derart mit Katzenhaaren verstopft, dass er sich kaum noch drehen konnte! Eine schnelle Reinigung mittels Computer-Staubsauger und einer Spraydose mit Pressluft machte meinen Kunden wieder zu einem zufriedenen Anwender.

Die CPU benötigt eine ausreichende Belüftung. Natürlich ist ein Lüfter obligatorisch, es muss aber auch möglich sein, die Abwärme im Inneren des Computergehäuses durch einen oder mehrere Lüfter hinauszubefördern und kühle Frischluft durch die Lüftungsschlitze anzusaugen. Bei Verstopfungen, defekten oder blockierten Lüftern kann sich das Gehäuseinnere so sehr erwärmen, dass die Kühlung wirkungslos bleibt. Das Resultat ist ein System, das sich spontan neustartet oder nur langsam arbeitet.

3.5.2 Totalausfall

Ein Totalausfall ist nicht zu übersehen. Der PC zeigt plötzlich einen *Blue Screen of Death* (*BSoD*), der formal als »Windows Stop Error« bezeichnet wird (Abbildung 3.48). macOS zeigt in diesem Fall ein sich drehendes regenbogenfarbenes Scheibchen, das einfach nicht mehr verschwinden will, oder löst eine sogenannte Kernel Panic aus (einen automatischen Neustart). (Die CompTIA spricht in solchen Fällen von *proprietären Absturzbildschirmen.*)

```
Es wurde ein Problem festgestellt. Windows wurde heruntergefahren, damit der
Computer nicht beschädigt wird.

PROCESS1_INITIALIZATION_FAILED

Wenn Sie diese Fehlermeldung zum ersten Mal angezeigt bekommen,
sollten Sie den Computer neu starten. Wenn diese Meldung
weiterhin angezeigt wird, müssen Sie folgenden Schritten
folgen:

Stellen Sie sicher, dass neue Hardware oder Software richtig installiert
ist. Fragen Sie Ihren Hardware- oder Softwarehersteller nach möglicher-
weise erforderlichen Windows-Updates, falls es sich um eine Neuinstallation
handelt.

Falls das Problem weiterhin bestehen bleibt, sollten Sie alle neu
installierte Hardware oder Software deinstallieren. Deaktivieren
Sie BIOS-Optionen wie Caching oder Shadowing. Starten Sie den Computer
neu, drücken Sie die F8-TASTE, um die erweiterten Startoptionen zu wählen,
und wählen Sie dann den abgesicherten Modus, falls Sie zum Löschen oder
Deaktivieren von Komponenten den abgesicherten Modus verwenden müssen.

Technische Information:

*** STOP: 0x0000006B (0xC0000018,0x00000005,0x00000000,0x00000000)
```

Abb. 3.48: Fehlermeldung bei Totalausfall

Vielleicht geht der PC auch plötzlich aus und der Bildschirm wird schwarz, begleitet von einem lauten Knall. Ihre olfaktorischen Sinne werden mit dem beißenden Geruch von durchgebrannter Elektronik oder Ozon verwöhnt. Es kann sogar vorkommen, dass Sie ein kleines Rauchwölkchen aus dem Gehäuse aufsteigen sehen. Sie können zwar nicht unmittelbar feststellen, ob der Prozessor abgeraucht ist, aber immer der Nase nach! Im Ernst: Schnüffeln Sie im Gehäuse herum, bis Sie die am stärksten riechende Stelle lokalisiert haben. Handelt es sich um die CPU, ist das vermutlich eine schlechte Nachricht. Wo immer auch ein Kurzschluss stattgefunden hat, er könnte auch das Mainboard in Mitleidenschaft gezogen haben und Sie haben nun einiges an Reparaturarbeiten zu erledigen.

Jenseits von A+

3.6 Intel Core M

Der Intel Core M bleibt ist sehr energieeffizient und wurde für den Einsatz in mobilen Geräten entwickelt, bei denen es auf eine lange Akkulaufzeit ankommt. Die offizielle *TDP* (*Thermal Design Power*, die maximale thermische Verlustleistung) beträgt nur 4,5 Watt. Vergleichen Sie das mit der für mobile Geräte ausgelegten Variante eines Core i7, die 57 Watt benötigt. Um das zu erreichen, geht Intel einen Kompromiss bei der Rechenleistung des Core M ein. Sie liegt etwas unterhalb derjenigen einer mobilen Version des Core i3 – genug, um einfache Büroarbeiten oder Ähnliches zu erledigen, aber nicht ausreichend, um ernsthaft zu spielen oder andere anspruchsvolle Anwendungen auszuführen. Andererseits erlaubt es der geringe Energieverbrauch den Herstellern, auf einen Lüfter zu verzichten und besonders flache und leichte Geräte zu konstruieren.

3.7 Wiederholung

3.7.1 Fragen

1. Welchen Sinn haben Register für die CPU?
   A. Die Register legen die Taktfrequenz fest.
   B. Die CPU verwendet die Register als temporären Speicherplatz für interne Befehle und Daten.
   C. Mit Registern kann die CPU das RAM adressieren.
   D. Über Register kann die CPU den Adressbus steuern.
2. Welche Funktion hat der externe Datenbus im PC?
   A. Der externe Datenbus legt die Taktfrequenz der CPU fest.
   B. Die CPU verwendet den externen Datenbus zur RAM-Adressierung.
   C. Der externe Datenbus ist ein Kanal für die Übertragung von Daten und Befehlen zwischen CPU und RAM.
   D. Die CPU verwendet den externen Datenbus zum Zugriff auf die Register.
3. Welche Funktion hat der Adressbus im PC?
   A. Der Adressbus ermöglicht der CPU die Kommunikation mit dem MCC.
   B. Der Adressbus ermöglicht dem MCC die Kommunikation mit dem RAM.
   C. Der Adressbus stellt einen Kanal für den Datenfluss und die Befehle zwischen der CPU und dem RAM dar.
   D. Der Adressbus ermöglicht der CPU den Zugriff auf die Register.
4. Welche der folgenden Begriffe sind ein Maß für die CPU-Geschwindigkeit?
   A. Megahertz und Gigahertz
   B. Megabytes und Gigabytes
   C. Megahertz und Gigabytes
   D. Frontside-Bus und Backside-Bus
5. Welche CPU-Funktion ermöglicht es dem Prozessor, mehrere Betriebssysteme gleichzeitig auszuführen?
   A. Taktvervielfachung
   B. Cache-Speicher
   C. Pipelining
   D. Unterstützung für Virtualisierung
6. In welchen Sockel könnten Sie einen Intel Core i5 einsetzen?
   A. Sockel LGA 2011
   B. Sockel LGA 1151
   C. Sockel C
   D. Sockel AM3+
7. Welche Funktion ermöglicht es einer Einzelkern-CPU, wie zwei CPUs zu arbeiten?
   A. Hyperthreading
   B. SpeedStep
   C. Virtualisierung
   D. x64

8. Welche Schritte sind erforderlich, um eine Core-i3-CPU auf einem FM2+-Mainboard zu installieren?
   - **A.** Hebel am ZIF-Sockel betätigen; CPU der Markierung entsprechend ausrichten; Kühlkörper und Lüfter montieren.
   - **B.** Hebel am ZIF-Sockel betätigen; CPU der Markierung entsprechend ausrichten; Wärmeleitpaste auftragen; Kühlkörper und Lüfter montieren.
   - **C.** Hebel am ZIF-Sockel betätigen; CPU der Markierung entsprechend ausrichten; Kühlkörper und Lüfter montieren; Lüfter anschließen.
   - **D.** Egal welche Schritte man durchführt, es wird nicht funktionieren.
9. Ein Kunde ruft an und beschwert sich darüber, dass sein Computer zwar startet, aber beim Hochfahren von Windows abstürzt. Nach einigen kurzen Fragen finden Sie heraus, dass sein Neffe ihm am Wochenende eine RAM-Erweiterung installiert hat und den Computer danach nicht mehr zum Laufen bekam. Was könnte hier das Problem sein?
   - **A.** Zersetzung der Wärmeleitpaste
   - **B.** Nicht angeschlossener Lüfter
   - **C.** Defekter CPU-Cache-Speicher
   - **D.** Das ist völlig normal, das RAM muss ein paar Tage »eingefahren« werden.
10. Daniel hat im Rechner eines Kunden eine neue CPU installiert. Beim Einschalten des Rechners geschieht jedoch gar nichts. Die LED auf dem Mainboard leuchtet jedoch, sodass er sich sicher sein kann, dass das System mit Strom versorgt wird. Was könnte hier das Problem sein?
    - **A.** Er hat vergessen, den Lüfter wieder anzuschließen.
    - **B.** Er hat vergessen, zwischen CPU und Kühlkörper Wärmeleitpaste aufzutragen.
    - **C.** Er hat eine AMD-CPU in ein Intel-Mainboard eingebaut.
    - **D.** Er hat eine Intel-CPU in ein AMD-Mainboard eingebaut.

3.7.2 Antworten

1. **B.** Die CPU verwendet die Register als temporären Speicher für interne Befehle und Daten.
2. **C.** Der externe Datenbus ist ein Kanal für die Übertragung von Daten und Befehlen zwischen CPU und RAM.
3. **A.** Der Adressbus ermöglicht der CPU die Kommunikation mit dem MCC (Memory Controller Chip, dt. Speicher-Controller-Chip).
4. **A.** Die Begriffe Megahertz (MHz) und Gigahertz (GHz) geben an, wie viele Millionen bzw. Milliarden Taktzyklen pro Sekunde eine CPU ausführen kann.
5. **D.** Intel- und AMD-CPUs bringen Unterstützung für Virtualisierung mit und ermöglichen dadurch eine effizientere Implementierung virtueller Maschinen.
6. **B.** Der Intel Core i5 findet sich in verschieden Sockeltypen, insbesondere im LGA 1150 und im LGA 1151.
7. **A.** Beim Hyperthreading kann ein Einzelkern-Prozessor wie ein Doppelkern-Prozessor arbeiten, sofern das Betriebssystem dies unterstützt.
8. **D.** Intel-Prozessoren und AMD-Mainboards sind nicht kompatibel.
9. **B.** Höchstwahrscheinlich hat der Neffe den Lüfter abgeklemmt, um an die RAM-Steckplätze zu gelangen, und einfach nur vergessen, ihn wieder anzuschließen.
10. **B.** Die beste Antwort ist hier wohl die vergessene Wärmeleitpaste, allerdings kommt der nicht angeschlossene Lüfter ebenfalls infrage.

RAM 4

Themen in diesem Kapitel:

- Verschiedene DRAM-Bauformen
- Die Eigenschaften von RAM
- Passendes RAM auswählen und installieren
- Fehlersuche bei RAM-Problemen

Immer wenn jemand auf mich zukommt und mit seinem Computerfachwissen prahlen will, dann stelle ich ein paar Fragen, um festzustellen, wie viel mein Gegenüber wirklich weiß. Sollten wir uns also jemals persönlich begegnen, dann sollten Sie zumindest meine beiden ersten Fragen beantworten können, wenn Sie sich auf ein technisches Geplänkel mit mir einlassen wollen. Beide beziehen sich auf das RAM (*Random Access Memory*), den Arbeitsspeicher der CPU.

1. »Wie viel Arbeitsspeicher besitzt Ihr Rechner?«
2. »Was ist Arbeitsspeicher überhaupt und warum ist es so wichtig, dass jeder PC über genügend RAM verfügt?«

Können Sie eine dieser beiden Fragen beantworten? Falls nicht, braucht Sie das aber auch nicht sonderlich zu stören, denn in diesem Kapitel werden Sie die Antworten erfahren. Wiederholen wir noch einmal, was wir bisher über RAM wissen.

Wenn Programme und Daten nicht benötigt werden, befinden sie sich auf Massenspeichern, bei dem es sich zwar meist um Festplatten, manchmal aber auch um USB-Laufwerke, optische Datenträger (CDs/DVDs) oder andere Geräte handelt, die Daten auch dann speichern können, wenn der Rechner ausgeschaltet ist. Wenn Sie in Windows auf ein Programmsymbol klicken, kopiert ihr PC das Programm vom Massenspeicher ins RAM und führt es dann aus (Abbildung 4.1).



Abb. 4.1: Programme werden zwar auf Massenspeichermedien gelagert, aber zur Ausführung ins RAM geladen.

In Kapitel 3, *Mikroprozessoren*, haben Sie erfahren, dass die CPU *DRAM* (*Dynamic Random Access Memory*) als Arbeitsspeicher in allen PCs verwendet. So wie die CPUs haben sich auch DRAM-Bausteine im Laufe der Jahre in zahlreichen Schritten weiterentwickelt, sodass immer bessere DRAM-Technologien mit Namen wie SDRAM, RDRAM und DDR RAM entstanden. Dieses Kapitel erklärt zunächst die Funktionsweise von DRAM. Anschließend werden die in den letzten Jahren verwendeten, verschiedenen DRAM-Typen und deren Vorteile beschrieben. Im dritten Abschnitt 4.3, *Der Umgang mit RAM*, finden Sie detaillierte Informationen zur Auswahl der richtigen RAM-Bausteine und deren Installation. Das Kapitel endet mit der Beschreibung der Fehlersuche bei RAM-Problemen.

Geschichte und Konzepte

4.1 DRAM – Einführung

Wie in Kapitel 3, *Mikroprozessoren*, bereits beschrieben, verhält sich DRAM ähnlich wie das elektronische Arbeitsblatt einer Tabellenkalkulation mit nummerierten Zeilen, die Zellen enthalten, wobei jede Zelle eine Eins oder eine Null enthalten kann. Jetzt sehen wir uns genauer an, was physisch passiert. Bei jeder Zelle des Arbeitsblatts handelt es sich um ein spezielles Halbleiterelement, das einen Wert (1 oder 0) enthalten kann und aus mikroskopisch kleinen Kondensatoren und Transistoren besteht. DRAM-Hersteller integrieren diese winzigen Halbleiter in Chips, die eine bestimmte Anzahl von Bits speichern können. Die Bits sind in den Chips in Zeilen und Spalten und damit in rechteckiger Form angeordnet.

Jeder Chip kann nur begrenzt viele Codezeilen aufnehmen. Stellen Sie sich eine Codezeile als eine Zeile des elektronischen Arbeitsblatts vor. Beispielsweise könnte ein Chip eine Million, ein anderer über eine Milliarde Zeilen speichern. Darüber hinaus gibt es bei allen Chips eine Begrenzung hinsichtlich der Breite der Codezeilen, die er speichern kann. Beispielsweise könnte ein Chip 8 Bit breite Daten, ein anderer 16 Bit breite Daten speichern. Techniker geben die Kapazität von Chips in Bits und nicht in Bytes an, also *x8* bzw. *x16*. So wie Sie ein Arbeitsblatt über die Anzahl an Zeilen und Spalten beschreiben können, beschreiben auch Speicherhersteller ihre RAM-Chips. Bei einem einzelnen DRAM-Chip, der 1.048.576 Zeilen und 8 Spalten speichern kann, würde es sich z.B. um einen *1M-x8*-Chip handeln, wobei »M« wie bei Megabyte (2^{20} Byte) als Abkürzung für »Mega« steht. Es ist schwierig, wenn nicht unmöglich, die Kapazität eines DRAM-Chips nur durch dessen Betrachtung festzustellen, denn nur die DRAM-Hersteller kennen die genaue Bedeutung der winzigen Ziffern auf den Chips, auch wenn man sie manchmal leicht erraten kann (siehe Abbildung 4.2).



Abb. 4.2: Was könnten diese Ziffern bedeuten?

Hinweis

Wahre RAM-Begeisterte finden auf den Websites der Hersteller ausführliche Einzelheiten über die Chips. Sehen Sie sich beispielsweise unter `http://www.micron.com/products/dram/ddr4-sdram/part-catalog` die Diagramme von Micron an.

4.1.1 DRAM-Organisation

DRAM ist seit Mitte der 1970er wegen seines günstigen Preises, seiner hohen Geschwindigkeit und seiner Fähigkeit, viele Daten auf relativ kleinem Raum zu speichern, zum Standard-RAM in allen Computern und nicht nur im PC geworden. DRAM begegnen Sie heute fast überall, z.B. in Autos und sogar in Backautomaten.

Das DRAM im PC muss genau definierten Anforderungen genügen. Der Original-8088 besaß einen 8-Bit-Frontside-Bus. Alle zum 8088-Prozessor übertragenen Befehle wurden in separate 8-Bit-Blöcke aufgeteilt. Sie brauchen daher RAM, das Daten in 8-Bit-Blöcken (1 Byte) speichern kann. Immer wenn also die CPU eine Codezeile anforderte, konnte der Speicher-Controller einen 8-Bit-Block auf den Datenbus schreiben. Damit wurde der Datenfluss in die CPU (und aus dieser heraus) optimiert. Auch wenn heutige DRAM-Chips breiter als 1 Bit sein können, waren anfangs alle DRAM-Chips nur 1 Bit breit. Dies bedeutet, dass die Kapazitäten bei 1 Bit Breite immer z.B. 64Kx1 oder 256Kx1 betrugen.

Wie kommt man dann aber mit 1 Bit breiten DRAMs zu 8 Bit breitem Speicher? Die Antwort ist eigentlich ganz einfach: Man nehme acht 1 Bit breite Chips und organisiere sie elektronisch über den über den *MCC* (*Memory Controller Chip, dt. Speicher-Controller-Chip*) so, dass sich 8 Bit breiter Speicher ergibt (Abbildung 4.3).

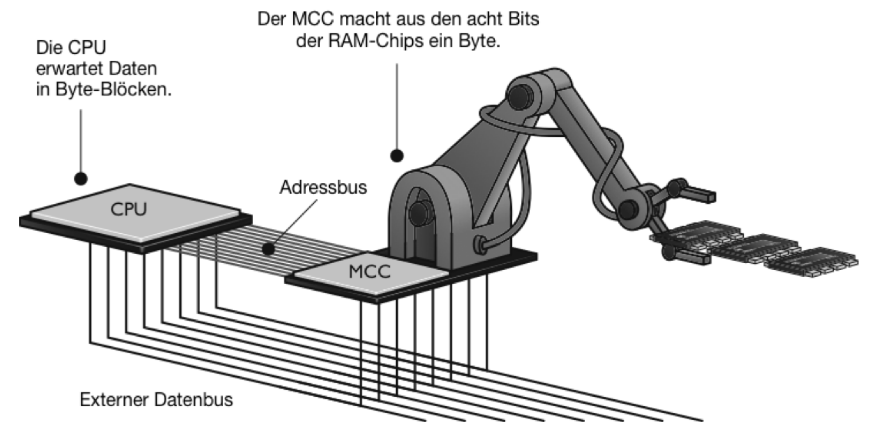
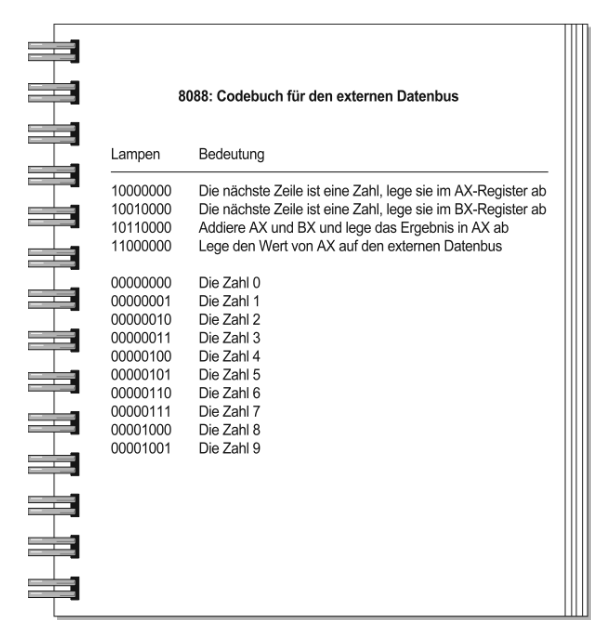


Abb. 4.3: Der MCC greift auf Daten in auf dem Mainboard aufgelöteten RAM-Chips zu.

4.1.2 DRAM in der Praxis

Bevor ich nun den nächsten Schritt erläutere, muss ein wichtiger Punkt geklärt werden. Als Sie im vorherigen Kapitel die Maschinensprache des 8088 kennengelernt haben, handelte es sich bei allen Beispielen aus dem Codebuch um 1-Byte-Befehle. Abbildung 4.4 zeigt noch einmal das Codebuch. Können Sie erkennen, dass alle Befehle 1 Byte lang sind?



8088: Codebuch für den externen Datenbus

Lampen	Bedeutung
10000000	Die nächste Zeile ist eine Zahl, lege sie im AX-Register ab
10010000	Die nächste Zeile ist eine Zahl, lege sie im BX-Register ab
10110000	Addiere AX und BX und lege das Ergebnis in AX ab
11000000	Lege den Wert von AX auf den externen Datenbus
00000000	Die Zahl 0
00000001	Die Zahl 1
00000010	Die Zahl 2
00000011	Die Zahl 3
00000100	Die Zahl 4
00000101	Die Zahl 5
00000110	Die Zahl 6
00000111	Die Zahl 7
00001000	Die Zahl 8
00001001	Die Zahl 9

Abb. 4.4: Noch einmal das Codebuch

Die Realität sieht ein wenig anders aus. Die meisten Befehle der 8088-Maschinensprache umfassen zwar wirklich ein Byte, für ein paar komplexere Befehle werden aber zwei Byte benötigt. Der nachfolgende Befehl sorgt z.B. dafür, dass sich die CPU 163 Byte im RAM-Arbeitsblatt »nach oben bewegt« und den Befehl ausführt, der sich dort befindet. Cool, oder?

```
1110100110100011
```

Das Problem dabei ist, dass der Befehl 2 Byte und nicht nur 1 Byte lang ist! Wie kommt der 8088 denn damit klar? Er übernimmt einfach nur jeweils ein Byte. Die Übernahme des Befehls dauert dann zwar doppelt so lange, da der MCC zwei Mal Daten aus dem Arbeitsspeicher holen muss, aber es funktioniert.

Wenn aber einige der Befehle mehr als 1 Byte umfassen, warum hat dann Intel den 8088 nicht mit einem 16-Bit-Frontside-Bus ausgestattet? Wäre das nicht besser? Genau das hat Intel auch gemacht! Intel hat den 8086-Prozessor entwickelt. Der 8086 ist eigentlich älter als der 8088 und war mit diesem, abgesehen von einem kleinen Detail, absolut identisch, denn er hatte einen 16-Bit-Frontside-Bus. Wenn Intel und IBM gewollt hätten, dann hätten sie den 8086 statt des 8088 und 2 Byte breites RAM anstelle des 1 Byte breitem RAM verwenden können. Natürlich hätten sie einen MCC entwickeln müssen, der mit derartigem RAM umgehen kann (siehe Abbildung 4.5).

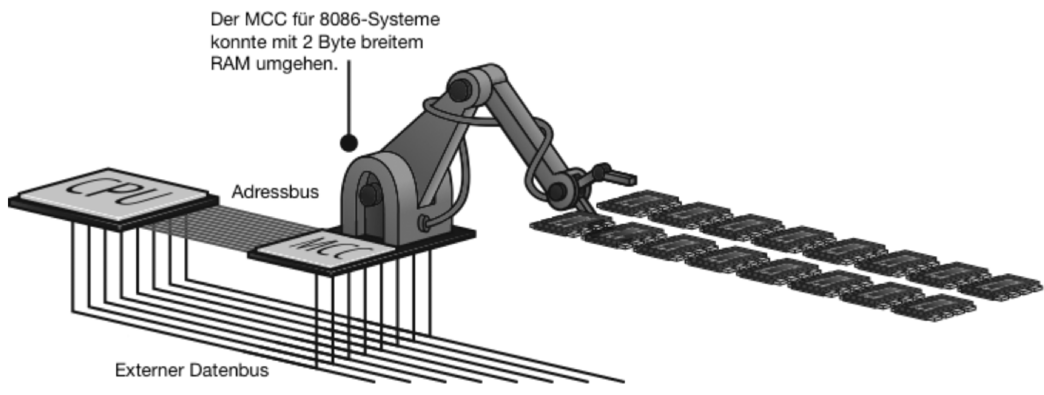


Abb. 4.5: Der aufgemotzte 8086-MCC bei der Arbeit

Warum also setzte IBM nicht den 8086 anstelle des 8088 ein? Speicher-Controller und Speicherbausteine, die mit 2 Bytes gleichzeitig umgehen konnten, waren damals noch kaum erschwinglich. Sicherlich gab es bereits entsprechende Chips, aber diese waren teuer und IBM konnte sich wahrscheinlich nicht vorstellen, dass jemand 12.000 Dollar (bzw. damals ca. 25.000 DM) für einen Personal Computer auszugeben bereit gewesen wäre. Also kaufte IBM den Intel 8088 und nicht den Intel 8086 und sprach den Arbeitsspeicher byteweise an. Wie Sie sich aber sicherlich vorstellen können, blieb das nicht lange so!

4.1.3 DRAM-Module

Mit zunehmender Größe des CPU-Datenbusses wuchs auch der Bedarf nach RAM, das breit genug war, um den Bus zu füllen. Die Intel-80386-CPU beispielsweise hatte einen 32-Bit-Datenbus und brauchte deshalb 32 Bit breites DRAM. Stellen Sie sich vor, Sie müssten 32 jeweils 1 Bit breite DRAM-Chips auf einem Mainboard unterbringen. Was für eine Platzverschwendung! Abbildung 4.6 zeigt ein Beispiel für Amok laufendes RAM auf dem Mainboard.

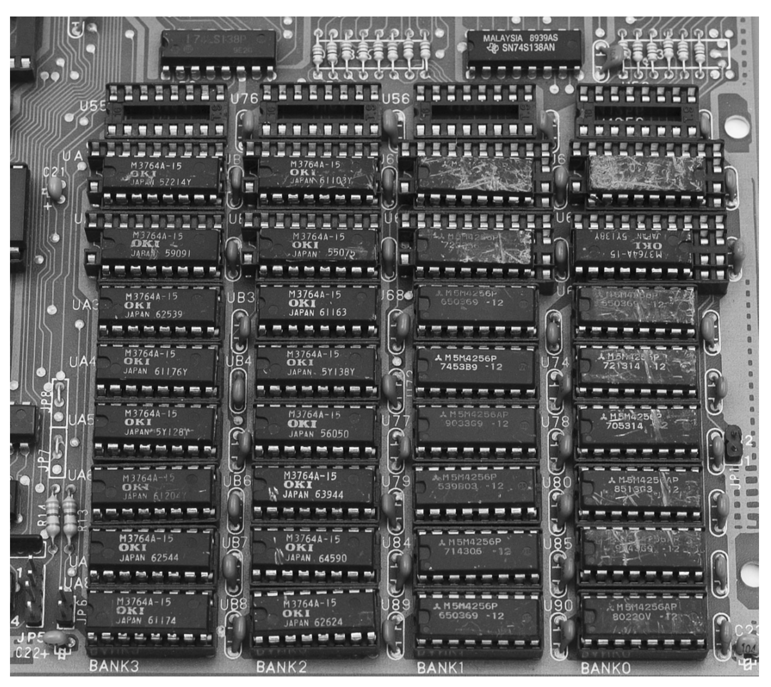


Abb. 4.6: Hier belegen die RAM-Chips eine Menge Platz auf dem Mainboard!

Die DRAM-Hersteller reagierten, indem sie breitere DRAM-Chips bauten, wie etwa x4, x8 und x16, und jeweils mehrere davon auf kleinen Platinen bzw. Speichermodulen anordneten. Abbildung 4.7 zeigt eins der ersten Module mit 8 DRAM-Chips, die *SIMM* (*Single Inline Memory Module*) genannt wurden. Um einem modernen System RAM hinzuzufügen, muss man die für das jeweilige Mainboard passenden Module auswählen. Im Mainboard-Handbuch finden Sie genauere Informationen darüber, welche Module verwendet werden können und wie viel RAM Sie installieren können.

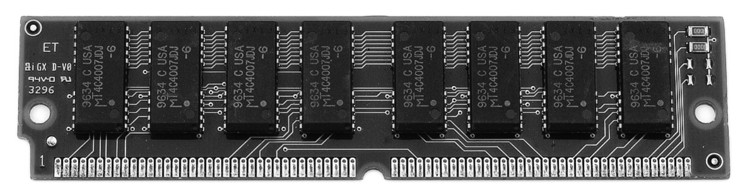


Abb. 4.7: Ein 72-poliges SIMM

Moderne CPUs sind sehr viel intelligenter als der betagte Intel 8088. Ihre Maschinensprachen enthalten Befehle, die bis zu 64 Bit (8 Byte) breit sind. Außerdem haben sie einen mindestens 64 Bit breiten Frontside-Bus, über den mehr als nur 8 Bit gleichzeitig übertragen werden können. Sie wollen kein läppisches 8-Bit-RAM! Um die Datenübertragung von und zu der CPU zu optimieren, liefern moderne Speicher-Controller mindestens 64 Bit Daten an, wenn die CPU Daten aus dem RAM anfordert.

Tipp: Alte RAM-Bausteine

In der PC-Welt halten ständig neue Technologien und Verfahren Einzug. Einem Techniker, der die alten Methoden kennt, stehen zusätzliche Möglichkeiten zur Verfügung. Tausende Unternehmen, wie Krankenhäuser, Autowerkstätten usw., nutzen sehr alte, proprietäre Anwendungen, um Krankenakten, Inventar

und dergleichen zu verwalten. Wenn man Sie bittet, für eines dieser betagten Systeme Support zu leisten, müssen Sie wissen, wie man mit den alten Bauteilen umgeht. Probieren Sie Folgendes aus:

Besorgen Sie sich einen alten Computer. Fragen Sie Ihren Onkel, Ihren Cousin oder Großtante Erna, ob sie noch einen alten PC besitzen, der auf dem Dachboden verstaubt, den Sie verwenden könnten. Sollte das nicht klappen, können Sie immer noch bei einem Gebrauchtwarenhändler für ein paar Euro einen alten PC erwerben.

Öffnen Sie das Gerät und überprüfen Sie den Arbeitsspeicher. Bauen Sie die RAM-Bausteine aus und wieder ein, um sich damit vertraut zu machen. Man kann nie wissen, ob nicht ein älteres betriebsnotwendiges System plötzlich ausfällt, das unverzüglich repariert werden muss – und zwar von Ihnen!

Moderne DRAM-Module gibt es in 32 und 64 Bit breiten Formfaktoren und mit unterschiedlich vielen Chips. Viele Techniker beschreiben diese Speichermodule über ihre Breite, wie also *x32* und *x64*. Beachten Sie, dass sich diese Zahlen *nicht* auf die Breite der einzelnen DRAM-Chips auf dem Modul beziehen. Wenn Sie etwas von irgendwelchem Speicher lesen oder hören, achten Sie einfach darauf, ob von der DRAM- oder der Modulbreite die Rede ist. Wenn die CPU bestimmte Datenbytes benötigt, dann fordert sie diese über den Adressbus an. Die CPU kennt weder die physische Position, an der diese Daten gespeichert sind, noch die physische RAM-Organisation (z.B. wie viele DRAM-Chips zusammenarbeiten, um die 64 Bit breiten Speicherzeilen zu bilden). Dafür ist der MCC zuständig, der den Arbeitsspeicher verwaltet und der CPU die jeweils angeforderten Bytes übergibt (Abbildung 4.8).

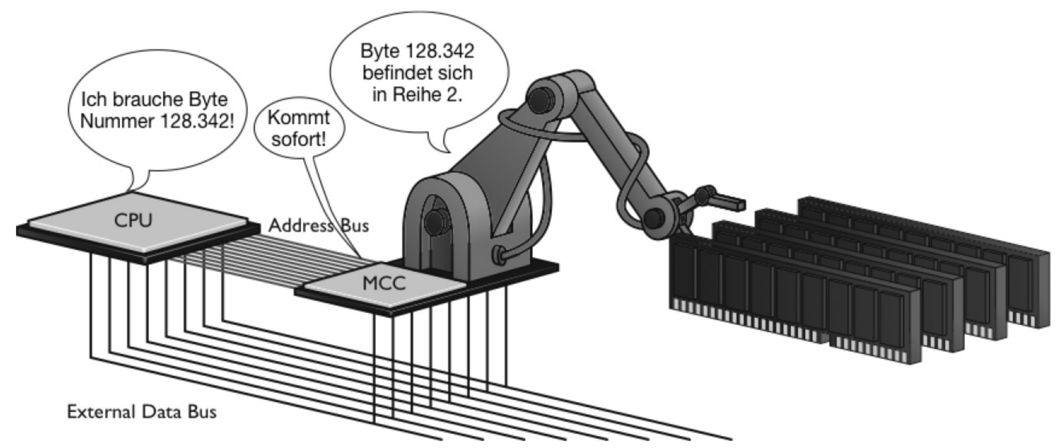


Abb. 4.8: Der MCC kennt die tatsächliche Position im DRAM.

4.1.4 Speichermodule für den Endkunden

Wenn moderne DRAM-Module sehr viel breiter als ein Byte sind, warum verwenden die Leute dann immer noch das Wort »Byte«, um auszudrücken, wie viel DRAM sie haben? Konvention. Gewohnheit. Statt eine Bezeichnung zu verwenden, die den elektronischen Aufbau des RAMs beschreibt, wird üblicherweise die *Gesamtspeicherkapazität des Moduls in Byte* angegeben. Beispielsweise könnte Ben sagen, er habe ein 8-GB-Speichermodul auf seinem Mainboard, während Sabine zwei 4-GB-Module hat. Beide Systeme besitzen insgesamt acht Gigabyte Arbeitsspeicher. Und genau das interessiert die Kunden, weil ihre Systeme schneller und stabiler laufen, wenn sie genügend Arbeitsspeicher besitzen. Ist zu wenig Arbeitsspeicher vorhanden, dann laufen die Systeme nicht optimal. Als Techniker müssen Sie natürlich mehr wissen, um die richtigen Module für die unterschiedlichsten Computer auswählen zu können.

4.2 RAM-Typen

Die Entwicklung neuer, breiterer und schnellerer CPUs und MCCs motivierte die DRAM-Hersteller, neue DRAM-Technologien zu erfinden, die bei einem einzigen Zugriff genügend Daten bereitstellen, um den Datenfluss von und zur CPU zu optimieren.

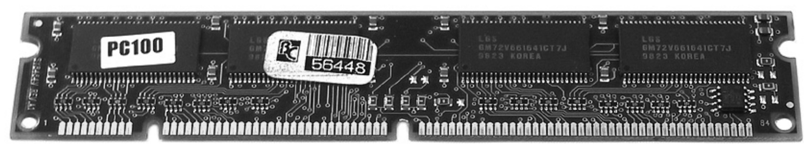
4.2.1 SDRAM

Die meisten modernen Systeme verwenden irgendeine Art von *synchronem* DRAM (SDRAM). SDRAM ist immer noch DRAM, aber es arbeitet synchron mit dem Systemtakt, so wie die CPU und der MCC, sodass der MCC weiß, wann Daten aus dem SDRAM übernommen werden können. Dadurch wird möglichst wenig Zeit vergeudet.

SDRAM gab es erstmals 1996 auf Modulen, die *DIMM* (*Dual Inline Memory Module*) genannt wurden. Die frühen SDRAM-DIMMs gab es mit unterschiedlich vielen Kontakten. Die gebräuchlichsten Varianten der Desktop-Rechner hatten 168 Pins. Die Laptop-DIMMS hatten 68, 144 (Abbildung 4.9) oder beim Mikro-DIMM 172 Kontakte, es gab sie aber auch als SO-DIMM (Small Outline DIMM) mit 72, 144 oder 200 Kontakten (Abbildung 4.10). Mit Ausnahme der 32 Bit breiten 72-Pin-SO-DIMMs arbeiteten all diese DIMM-Varianten mit 64 Bit Datenbreite, was dem 64-Bit-Datenbus aller CPUs seit dem Pentium entspricht.



Abb. 4.9: 144-Pin-Mikro-DIMM (Foto mit freundlicher Genehmigung von Micron Technology, Inc.)



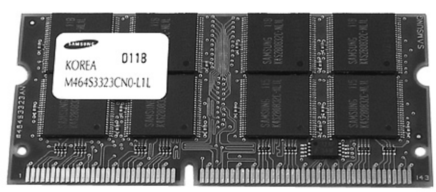


Abb. 4.10: Ein 168-Pin-DIMM (oben) und ein 144-Pin-SO-DIMM

Um SDRAM nutzen zu können, musste man einen PC haben, der das unterstützte. Wenn Sie beispielsweise ein System mit Steckplätzen für 168-Pin-DIMMs hatten, verwendete Ihr System SDRAM. Ein DIMM in einem dieser DIMM-Steckplätze konnte den 64-Bit-Bus auslasten, deshalb nannte man die einzelnen Steckplätze *Speicherbank* oder auch nur *Bank*. Man konnte ein, zwei oder mehrere Modul(e) installieren, und das System funktionierte. Beachten Sie, dass man bei Laptops, die mit 72-Pin-SO-DIMMs arbeiteten, die RAM-Module immer paarweise installieren musste, um eine Bank zu füllen, weil die einzelnen Module nur die halbe Busbreite boten. (In diesem Fall gehören zu einer Bank jeweils zwei Modulsteckplätze!)

SDRAM war mit dem Systemtakt verknüpft, sodass seine Taktgeschwindigkeit der des Frontside-Busses entsprach. Bei frühen SDRAM-Systemen waren fünf Taktgeschwindigkeiten gebräuchlich: 66, 75, 83, 100 und 133 MHz. Der Speichertakt musste mindestens so hoch wie der Systemtakt sein, sonst lief der Rechner instabil oder gar nicht mehr. Den Taktgeschwindigkeiten wurde, nach einem von Intel vorangetriebenen Standard, ein »PC« vorangestellt. Für die SDRAM-Geschwindigkeiten ergab sich daraus also PC66 bis PC133. Für einen Pentium-III-Rechner mit einem Frontside-Bustakt von 100 MHz musste man SDRAM-DIMMS kaufen, die für diesen geeignet waren, also z.B. PC100 oder PC133.

4.2.2 RDRAM

Als Intel den Pentium 4 entwickelte, wusste man, dass herkömmliche SDRAM-Bausteine für den mit vierfachem Systemtakt (quad-pumped) arbeitenden 400-MHz-Frontside-Bus einfach nicht schnell genug waren. Intel verkündete daher, dass es SDRAM durch eine sehr schnelle, neue Speichervariante ersetzen wollte, die von der Firma Rambus entwickelt worden war und *Rambus DRAM* oder einfach *RDRAM* genannt wurde (Abbildung 4.11). Das als nächster großer Wurf in der DRAM-Technologie angepriesene RDRAM unterstützte Geschwindigkeiten bis maximal 800 MHz und bot Intel reichlich Spielraum zur Verbesserung des Pentium 4.



Abb. 4.11: RDRAM

RDRAM wurde von der Industrie jahrelang mit Spannung erwartet. Die Unterstützung ließ dann aber zu wünschen übrig, da sich die Entwicklung stark verzögerte und der Preis schließlich weit über dem von SDRAM lag. RDRAM wurde schließlich nur widerwillig unterstützt, auch wenn nahezu alle PC-Hersteller eine Zeit lang Systeme mit RDRAM angeboten haben. Aus technischer Sicht besitzt RDRAM fast dieselben Merkmale wie SDRAM. Ein RDRAM-Speichermodul wird *RIMM* genannt. Dabei haben die Zeichen keine wirkliche Bedeutung, sondern reimen sich einfach nur mit SIMM und DIMM.

Hinweis

Die 400-MHz-Geschwindigkeit des Frontside-Busses wurde nicht über einen höheren Systemtakt erreicht, sondern dadurch, dass die CPU und der MCC in einem Taktzyklus zwei oder vier Mal 64 Bit Daten übertragen konnten, was letztlich einer effektiven Verdopplung oder Vervierfachung der Taktgeschwindigkeit des Systembusses entsprach.

1001

4.2.3 DDR-SDRAM

AMD und viele andere bedeutende System- und Speicherhersteller unterstützten und förderten *DDR-SDRAM* (*Double Data Rate SDRAM*). Grundsätzlich kopierte DDR-SDRAM Rambus. Dabei wird, wie der Name schon sagt, der Durchsatz des SDRAM einfach dadurch verdoppelt, dass je Taktzyklus zwei Verarbeitungsschritte erfolgen. Das passte hervorragend zum double-pumped Frontside-Bus beim Athlon und den nachfolgenden AMD-Prozessoren. DDR-SDRAM war zwar nicht so schnell wie RDRAM, aber dieser Aspekt war angesichts relativ niedriger Geschwindigkeiten des Frontside-Busses ohnehin fragwürdig. DDR-SDRAM war aber nur wenig teurer als das herkömmliche SDRAM.

DDR-SDRAM wird für Desktop-Rechner in Form 184-poliger DIMMs angeboten, deren physische Abmessungen zwar denen der normalen 168-poligen SDRAM-DIMMs entsprechen, die aber nicht pinkompatibel sind (Abbildung 4.12). Die Steckplätze der beiden RAM-Typen sehen zwar ähnlich aus, besitzen aber unterschiedliche Führungsnasen und Aussparungen, damit die beiden Typen nicht versehentlich verwechselt und in den falschen Steckplatz eingesetzt werden können. Bei Laptops werden für DDR-SDRAM entweder 200-polige SO-DIMMs oder 172-polige Micro-DIMMs verwendet (Abbildung 4.13).

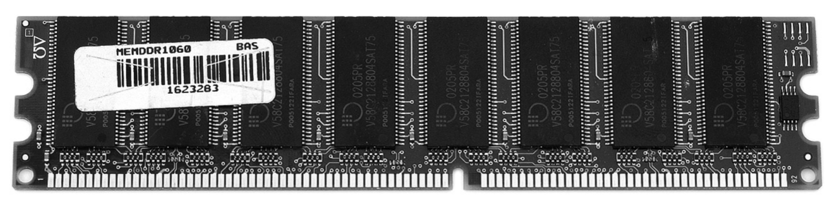


Abb. 4.12: DDR-SDRAM

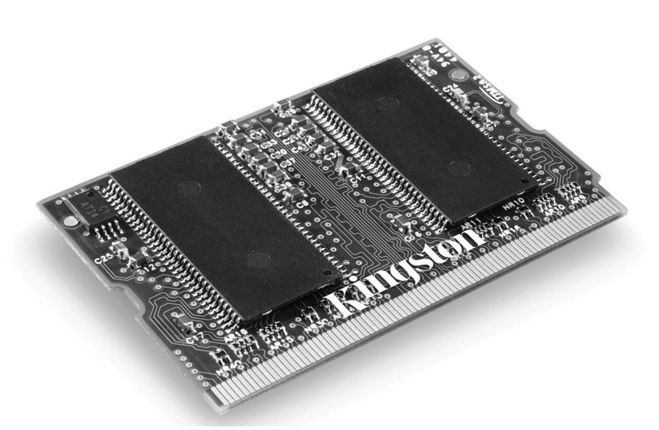


Abb. 4.13: 172-poliger DDR-SDRAM-Micro-DIMM
(Abbildung mit freundlicher Genehmigung von Kingston/Joint Harvest)

> **Hinweis**
>
> Die meisten Techniker lassen den SDRAM-Teil von DDR-SDRAM einfach ganz oder teilweise weg, wenn sie sich miteinander unterhalten. Man spricht vom Speicher als DDR, DDR-RAM und der interessanten Mischform DDRAM.

Bei DDR-Modulen werden einige durchaus interessante Namenskonventionen verwendet, die auf der maximalen Datenrate des RAMs in Bytes pro Sekunde basieren. Um die zu ermitteln, nehmen Sie die MHz-Geschwindigkeit und multiplizieren sie mit 8 Bytes (der Breite aller DDR-SDRAM-Sticks). 400 MHz multipliziert mit 8 ergibt 3200 Megabyte pro Sekunde (MBps). Dann setzen Sie noch die Abkürzung »PC« davor und erhalten die neue Bezeichnung PC3200. Viele Techniker verwenden auch die für die einzelnen DDR-Chips verwendete Namenskonvention. Beispielswiese bezieht sich DDR400 auf einen DDR-SDRAM-Chip mit 400 MHz, der mit einem Takt von 200 MHz läuft.

Auch wenn die Bezeichnung DDRxxx eigentlich nur für einzelne DDR-Chips vorgesehen ist und der Begriff PCxxxx für DDR-Module, wird es durch diese Tradition der zwei Namen für die RAM-Geschwindigkeiten etwas schwierig, weil die beiden Bezeichnungen austauschbar sind. Tabelle 4.1 führt alle DDR-Geschwindigkeiten auf, auch wenn sie teilweise nicht wirklich gebräuchlich sind.

Taktrate	DDR-Bezeichnung	PC-Bezeichnung
100 MHz	DDR200	PC1600
133 MHz	DDR266	PC2100
166 MHz	DDR333	PC2700
200 MHz	DDR400	PC3200
217 MHz	DDR433	PC3500
233 MHz	DDR466	PC3700
250 MHz	DDR500	PC4000
275 MHz	DDR550	PC4400
300 MHz	DDR600	PC4800

Tabelle 4.1: DDR-Geschwindigkeiten

Angeführt von AMD und anderen Herstellern übernahm die PC-Industrie DDR-SDRAM als Arbeitsspeicherstandard. Intel gab nach und stellte im Sommer 2003 die Produktion von Mainboards und Speicher-Controllern für RDRAM ein.

Auf eines kann man sich bei PC-Technologien verlassen – jede gute Idee, die kopiert werden kann, wird auch kopiert. Eines der besten Konzepte von Rambus war die Zweikanal-Architektur (»Dual Channel«), bei der zwei RDRAM-Module kombiniert für eine höhere Datenrate sorgen. Die Hersteller haben Mainboards mit MCCs entwickelt, die die Zweikanal-Architektur der DDR-SDRAMs unterstützen. Zweikanal-DDR-Mainboards verwenden reguläre DDR-Module, auch wenn die Hersteller RAM häufig paarweise aufeinander abgestimmt verkaufen und sie Dual-Channel-RAM nennen.

Tipp

Sehen Sie sich die Übung für Kapitel 4 zur Berechnung von RAM-Geschwindigkeiten unter `http://totalsem.com/100x` an!

Dual-Channel-RAM benötigt zwei identische DDR-Module, die paarweise in die Steckplätze eingesetzt werden müssen. Auf vielen Mainboards gibt es vier Steckplätze (siehe Abbildung 4.14).



Abb. 4.14: Ein Mainboard mit vier RAM-Steckplätzen. Die jeweils gleichfarbigen Steckplätze müssen mit gleichartigen Modulen bestückt werden, wenn das Mainboard den Zweikanalmodus nutzen soll.

4.2.4 DDR2

Bei *DDR2* handelt es sich um DDR-RAM mit einigen Verbesserungen hinsichtlich der elektrischen Eigenschaften, sodass es noch schneller als DDR ist und dabei weniger Energie verbraucht. Die größte Geschwindigkeitssteigerung bei DDR2 resultiert aus der Taktverdopplung der E/A-Schaltkreise auf dem Chip. Damit wird der Kernspeicher, der die Daten aufnimmt, zwar nicht schneller, aber durch die beschleunigte Ein-/Ausgabe und zusätzlichen schnellen Pufferspeicher (vergleichbar mit einem Cache) ist DDR2 deutlich schneller als DDR. Für DDR2 werden 240-polige DIMMs verwendet, die nicht mit DDR kompatibel sind (Abbildung 4.15). Und auch die 200-poligen DDR2-SO-DIMMs sind mit den DDR-SO-DIMMs nicht kompatibel. Es gibt Mainboards, die sowohl Einkanal- als auch Zweikanal-DDR2 unterstützen.



Abb. 4.15: 240-poliges DDR2-DIMM

Hinweis

DDR2-Speichermodule passen nicht in DDR-Steckplätze und sind mit diesen auch elektronisch nicht kompatibel.

In Tabelle 4.2 sind einige der gängigen DDR2-Geschwindigkeiten aufgeführt.

Kernspeichertakt	DDR-E/A-Geschwindigkeit	DDR2-Angabe	PC-Angabe
100 MHz	200 MHz	DDR2-400	PC2-3200
133 MHz	266 MHz	DDR2-533	PC2-4200
166 MHz	333 MHz	DDR2-667	PC2-5300
200 MHz	400 MHz	DDR2-800	PC2-6400
266 MHz	533 MHz	DDR2-1066	PC2-8500

Tabelle 4.2: DDR2-Geschwindigkeiten

4.2.5 DDR3

DDR3 sorgt noch einmal für mehr Geschwindigkeit, besitzt eine effizientere Architektur und verbraucht etwa 30 Prozent weniger Energie. Wie bei den Vorgängern werden auch für DDR3 240-polige DIMMs verwendet, die aber wieder anders geformt sind, damit Benutzer allenfalls mit roher Gewalt (und einem Hammer) die falschen Speichermodule in ihre Systeme einbauen können (Abbildung 4.16). DDR3-SO-DIMMs für tragbare Computer besitzen 204 Kontakte und passen auch nicht in die älteren DDR2-Steckplätze.



Abb. 4.16: DDR2-DIMM auf einem DDR3-DIMM

Wichtig

In der Prüfung 220-1001 werden Ihre Kenntnisse der verschiedenen RAM-Typen wie DDR2, DDR3 und DDR4 abgefragt. Vergewissern Sie sich, dass Sie die individuellen Eigenschaften und die Unterschiede kennen. DDR3-DIMMs besitzen 240 Pins, DDR3-SO-DIMMS hingegen 204.

Hinweis

Verwechseln Sie DDRx nicht mit GDDRx. GDDRx wird nur für Grafikkarten verwendet. In Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*, erfahren Sie mehr über die verschiedenen Speichertypen auf Grafikkarten.

Bei DDR3 wird der Puffer des DDR2-Speichers von vier auf acht Bit erweitert, was für eine riesige Steigerung der Bandbreite im Vergleich mit älterem RAM sorgt. Und nicht nur das, einige DDR3-Module (und neuere) besitzen eine sogenannte *XMP*-Funktion (*eXtended Memory Profile*), mit deren Hilfe erfahrene Benutzer ihren Arbeitsspeicher leicht übertakten können, um den ohnehin schon schnellen Speicher weiter zu beschleunigen. Die Speicherchips auf DDR3-Modulen sind zudem dichter gepackt und es gibt DDR3-Module mit bis zu 16 GB Speicherkapazität. AMDs Version von XMP heißt AMP (*AMD Memory Profile*).

Einige Chipsätze für DDR3 unterstützen auch einen Drei- oder Vierkanalbetrieb (*Tripel-Channel- oder Quad-Channel-Architektur*), der dem älteren Zweikanalbetrieb des Speichers ähnelt, an dem aber drei

oder vier und nicht mehr zwei RAM-Module beteiligt sind. Neuere Intel- und AMD-Systeme verwenden wieder die Zweikanal-Architekur, aber es gibt noch viele Systeme, die den Drei- oder Vierkanalbetrieb unterstützen.

Wichtig

Machen Sie sich mit den Single-, Dual-, Tripel- und Quad-Memory-Architekturen vertraut.

In Tabelle 4.3 sind die verbreiteten DDR3-Geschwindigkeiten aufgeführt. Beachten Sie, dass die DDR3-E/A-Geschwindigkeiten jeweils dem vierfachen Kernspeichertakt entsprechen, während sie bei DDR2 nur doppelt so hoch waren. Diese Geschwindigkeitssteigerung lässt sich auf den größeren Puffer zurückführen, durch den DDR3 mit jedem Taktzyklus doppelt so viele Daten wie DDR2 übernehmen kann.

Kernspeichertakt	DDR-E/A-Geschwindigkeit	DDR3-Angabe	PC-Angabe
100 MHz	400 MHz	DDR3-800	PC3-6400
133 MHz	533 MHz	DDR3-1066	PC3-8500
166 MHz	667 MHz	DDR3-1333	PC3-10667
200 MHz	800 MHz	DDR3-1600	PC3-12800
233 MHz	933 MHz	DDR3-1866	PC3-14900
266 MHz	1066 MHz	DDR3-2133	PC3-17000
300 MHz	1200 MHz	DDR3-2400	PC3-19200

Tabelle 4.3: DDR3-Geschwindigkeiten

4.2.6 DDR3L/DDR3U

Die Speicherhersteller bietet eine DDR3-Version an, die mit geringerer Spannung betrieben und am häufigsten als *DDR3L* bezeichnet wird. Bei RAM-Anwendungen großen Umfangs können dadurch beträchtliche Kosten eingespart werden. (Denken Sie hier an richtig große Datencenter wie bei Google.) DDR3L verwendet eine Spannung von 1,35 Volt (V), während herkömmliches DDR3 1,5 bis 1,65 V nutzt – eine Einsparung von bis zu 15%, die sich schnell summiert. Die mit noch geringerer Spannung betriebene DDR3-Version *DDR3U* kommt sogar mit sparsamen 1,25 V aus.

Geringere Spannung bedeutet, dass weniger Wärme erzeugt wird. Bei einer Serverfarm oder einem Datencenter senkt das die Kosten für die Klimatisierung erheblich – eine feine Sache.

Die DDR3- und DDR3L-Steckplätze sind zwar mechanisch kompatibel, das heißt aber nicht, dass man auf älteren Mainboards die DDR3-Module einfach durch DDR3L-Module ersetzen kann. Wenn das Mainboard die Steckplätze mit einer Spannung von 1,5 V versorgt, die RAM-Module aber für 1,35 V ausgelegt sind, wird das womöglich zu Problemen führen.

Am besten studieren Sie das Handbuch des Mainboard-Herstellers oder sehen auf dessen Website nach. Viele Speicherhersteller bieten auch RAM-Module an, die sowohl mit 1,35 als auch mit 1,5 V betrieben werden können. Diese Bausteine funktionieren in allen Mainboards, die DDR3 unterstützen. Einige Module decken sogar das gesamte Spektrum von 1,25 bis 1,65 V ab.

4.2.7 DDR4

DDR4 wurde Ende 2014 mit viel Brimborium vorgestellt, hat sich aber nur langsam verbreitet. DDR4 bietet gegenüber DD3 eine höhere Speicherdichte, arbeitet mit geringerer Spannung und kann mit schnelleren Datentransferraten umgehen. Theoretisch könnten die Speicherhersteller DDR4-DIMMs

mit bis zu 512 GB produzieren. Derzeit besitzen die größten DDR4-Module eine Kapazität von 64 GB (im Gegensatz zu den 16 GB von DDR3), verwenden aber eine Spannung von nur 1,2 V. (Es gibt auch eine leistungsfähigere Variante, die mit 1,35 V betrieben wird sowie eine Niederspannungsversion, die 1,05 V nutzt.)

Bei DDR4 kommen DIMMs mit 288 Pins zum Einsatz, sie sind also nicht abwärtskompatibel zu DD3-Steckplätzen. DDR4-SO-DIMMs besitzen 260 Pins, die ebenfalls nicht in die Steckplätze für DD3-SO-DIMMs mit 204 Pins passen. Einige Hersteller bieten Mainboards an, die beide Steckplatztypen besitzen, um sowohl DDR3 als auch DDR4 zu unterstützen.

Hinweis

Wenn Sie das hier lesen, gibt es vielleicht schon DDR4-Module mit größerer Kapazität als 64 GB. Sehen Sie unter `http://www.newegg.com` nach.

Seit es DDR4 gibt, verwenden viele Techniker Megatransfers pro Sekunde (MT/s) als Maßeinheit für Datenübertragungen. Damit wird die Bandbreite als die Anzahl der in einer Sekunde stattfindenden Datentransferoperationen beschrieben. Für DDR4 ist dieser Wert ziemlich groß. In Tabelle 4.4 sind die gängigen DDR4-Geschwindigkeiten und die dazugehörigen Bezeichnungen aufgeführt.

Taktrate	Bandbreite	DDR4-Angabe	PC-Angabe
200 MHz	1600 MT/s	DDR4-1600	PC4-12800
266 MHz	2133 MT/s	DDR4-2133	PC4-17000
300 MHz	2400 MT/s	DDR4-2400	PC4-19200
400 MHz	3200 MT/s	DDR4-3200	PC4-25600
...			
563 MHz	4500 MT/s	DDR4-4500	PC4-36000
575 MHz	4600 MT/s	DDR4-4600	PC4-36800
588 MHz	4700 MT/s	DDR4-4700	PC4-37600

Tabelle 4.4: Standard-DDR4-Varianten

Wichtig

In der CompTIA-A+-Prüfung 1001 kommen lediglich DDR2-, DDR3- und DDR4-Module vor. DDR, DDR3L oder DDR3U bleiben außen vor.

4.2.8 RAM-Varianten

Innerhalb jeder RAM-Klasse gibt es Variationen in Hinblick auf Bauform, Geschwindigkeit, Qualität und die Verarbeitung mehr oder weniger fehlerhafter Daten. Systeme aus dem Profibereich benötigen häufig auch qualitativ hochwertigeres RAM, deshalb sollten Techniker diese Varianten kennen.

Doppelseitig bestückte DIMMs

Alle Arten von RAM-Modulen sind in zwei Varianten erhältlich: *einseitig* und *beidseitig bestückt*. Wie bereits aus der Bezeichnung hervorgeht, befinden sich bei den einseitig bestückten Modulen die Chips nur auf einer Seite der Platine, während sie bei den beidseitig bestückten Modulen auf beiden Seiten der Platine aufgelötet sind (Abbildung 4.17). Bei den doppelseitig bestückten Modulen handelt es sich im Grunde genommen um zwei RAM-Module, die auf eine Platine gelötet werden. Daran wäre

eigentlich auch nichts auszusetzen, wenn es nicht einige Mainboards gäbe, die mit den beidseitig bestückten Modulen entweder überhaupt nicht klarkommen oder diese nur einzeln oder in bestimmten Steckplätzen akzeptieren.

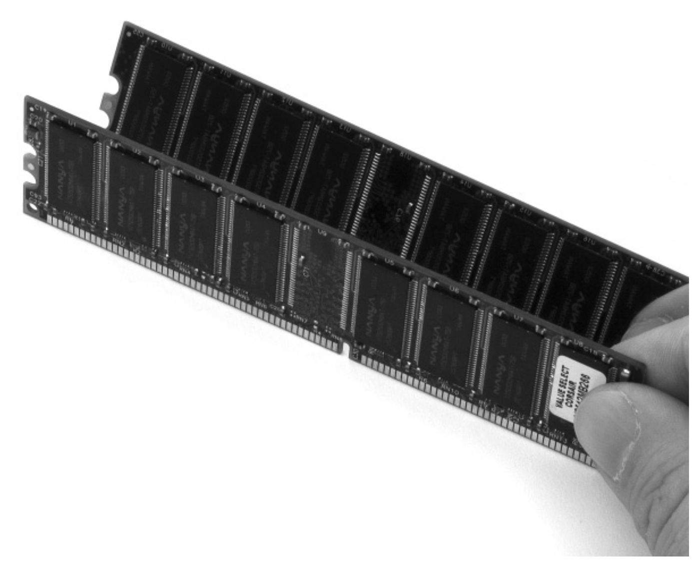


Abb. 4.17: Doppelseitig bestücktes DDR-SDRAM

Latenz

RAM reagiert unterschiedlich schnell auf elektrische Signale. Wenn beispielsweise der Speicher-Controller beginnt, eine Codezeile aus dem Speicher zu holen, kommt es zu einer leichten Verzögerung. Man kann es sich so vorstellen, als müsste das RAM erst einmal vom Sofa aufstehen. Nachdem das RAM die angeforderte Speicherzeile übertragen hat, gibt es erneut eine kleine Verzögerung, bevor der Speicher-Controller die nächste Zeile anfordern kann – das RAM hat sich sozusagen wieder hingesetzt. Die Verzögerungen aufgrund von Reaktionszeiten des RAMs werden auch *Latenz* genannt. Dafür gibt es Abkürzungen wie CL17 oder CL19, die Buchstaben der technischen Bezeichnung verwenden: *Column Array Strobe (CAS) Latency*.

RAM mit einer geringeren Latenz – wie beispielsweise CL17 – ist schneller als RAM mit einer höheren Latenz – wie beispielsweise CL19 –, weil es schneller antwortet. Die CL-Werte beziehen sich dabei auf die Anzahl der Taktzyklen, die bis zur Reaktion verstreichen. Die 17 bedeutet, dass der Speicher 17 Taktzyklen benötigt, bis er die angeforderten Daten abliefern kann, bei CL19 sind es 19. Da sich die Werte auf Taktzyklen beziehen, dauert eine Verzögerung von 19 Zyklen bei einer niedrigen Taktrate länger als bei einer hohen.

Hinweis

Die Latenzwerte geben an, wie viele Taktzyklen verstreichen, bis das RAM reagiert. Wenn Sie den Takt erhöhen, beispielsweise von 200 MHz auf 266 MHz, benötigt dasselbe RAM-Modul womöglich einen Taktzyklus länger, bevor es antwortet. Wenn Sie RAM-Module eines älteren Systems in ein neueres einsetzen, funktioniert das möglicherweise nicht, obwohl die RAM-Bausteine in die Steckplätze passen. Viele Mainboards gestatten es jedoch, das RAM-Timing manuell anzupassen. Versuchen Sie in diesem Fall, die Latenz ein wenig zu erhöhen, um dem langsameren RAM Zeit zum Antworten zu geben. In Kapitel 5, *BIOS und CMOS*, erfahren Sie, wie man solche Anpassungen vornimmt und wie Sie Ihr System wiederherstellen, falls Ihnen dabei ein Fehler unterläuft.

Als DDR2 und DDR3 aktuell waren, hatten diese Latenzwerte große Bedeutung. Spieler oder andere PC-Enthusiasten zahlten beträchtlich mehr für RAM mit niedriger Latenz. Als DDR4 auf den Markt kam, beschwerten sich Enthusiasten über die relativ hohe Latenz bei den Speicherherstellern und beklagten, dass es zu langsam sein würde. Nach Verfügbarkeit und ersten Tests zeigte sich jedoch, dass DDR4 dank der höheren Taktgeschwindigkeit genauso schnell war wie DDR3, selbst trotz der größeren Latenz. Man sollte beim Kauf von RAM durchaus auf die Latenz achten, sie ist heutzutage jedoch von sehr viel geringerer Bedeutung.

Aus technischer Sicht kann man sagen, dass einfach der richtige Speicher für das jeweilige System erforderlich ist. Wenn Sie ein Modul mit hoher Latenz in ein auf geringe Latenz ausgerichtetes Mainboard einsetzen, dann wird der Rechner instabil oder funktioniert gar nicht mehr. Lesen Sie im Handbuch für das Mainboard nach und beschaffen Sie sich die schnellsten vom Mainboard unterstützten Module. Dann sollte alles in Ordnung sein.

Parität und ECC

Angesichts der hohen Geschwindigkeiten und phänomenalen Datenmengen, die von typischen DRAM-Chips transportiert werden, kommt es gelegentlich vor, dass fehlerhafte Daten an den Speicher-Controller weitergegeben werden. Das bedeutet nicht unbedingt, dass das RAM defekt ist. Es könnte ein gelegentlicher Schluckauf sein, der durch irgendein unbekanntes Ereignis verursacht wurde, das einen intakten DRAM-Chip veranlasst, ein Bit als Null zu erkennen, obwohl es sich in Wahrheit um eine Eins handelt. Größtenteils bemerkt man es nicht einmal, wenn dieser seltene Fall eintritt. In einigen Umgebungen sind jedoch auch diese seltenen Ereignisse nicht tolerabel. Einem Bank-Server beispielsweise, der in der Sekunde Tausende von Online-Transaktionen verarbeitet, darf nicht der kleinste Fehler unterlaufen. Diese wichtigen Computer brauchen ein robusteres RAM, das absolut fehlerfrei funktioniert.

Der erste Typ des fehlertoleranten RAM wurde *Parity-RAM* oder *RAM mit Parität* genannt (Abbildung 4.18). Beim Parity-RAM wurde ein zusätzliches Datenbit (ein Paritätsbit) gespeichert, das der MCC zur Prüfung der Fehlerfreiheit der Daten verwenden konnte. Die Paritätsprüfung war nicht perfekt, denn damit ließen sich keineswegs alle Fehler erkennen, und zudem konnte der MCC erkannte Fehler auch nicht korrigieren. Jahrelang war die Paritätsprüfung das einzige Verfahren zum Aufspüren von Speicherfehlern.

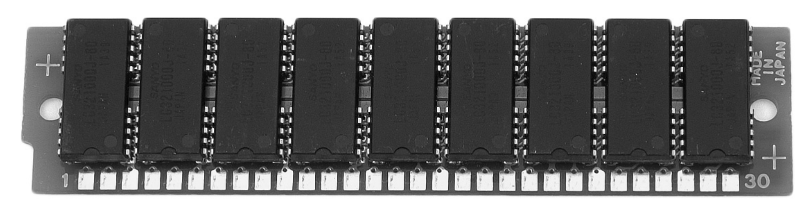


Abb. 4.18: Altes Modul mit Paritätsprüfung

Die heutigen PCs, die auf RAM-Fehler achten müssen, verwenden sogenanntes *ECC-RAM* (*Error Correction Code*) . ECC ist ein wesentlicher Fortschritt gegenüber der Fehlerprüfung von DRAM. ECC erkennt jedes fehlerhafte Bit und korrigiert diese Fehler in Echtzeit. Doppelte Bitfehler werden zwar erkannt, können aber *nicht* korrigiert werden. Die Überprüfung und Korrektur haben jedoch ihren Preis, denn ECC-RAM ist immer langsamer als RAM ohne Fehlerkorrekturschaltung.

ECC-DRAM gibt es in jeder DIMM-Bauform und kann zu den seltsamsten Chipbezeichnungen führen. Es gibt z.B. 240-polige DDR2-, DD3- (Abbildung 4.19) oder DDR4-Module in 72-Bit-Varianten und 200-polige Module im 72-Bit-SO-DIMM-Format. Die zusätzlichen 8 Bits jenseits der für die eigentlichen Daten benötigten 64 Bits werden für ECC verwendet.

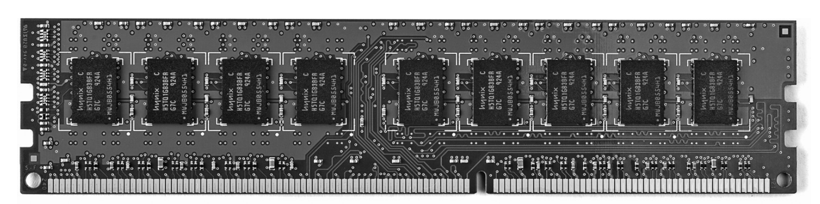


Abb. 4.19: ECC DDR3-Modul mit 9 Speicherchips

Sie könnten versucht sein, zu sagen, »So, jetzt probiere ich dieses ECC-RAM aus!« Tun Sie das nicht. Um ECC-RAM nutzen zu können, muss es auch vom MCC auf dem Mainboard unterstützt werden. Nur teure Mainboards für Profisysteme nutzen ECC. Und weil ECC nur in Sonderfällen benutzt wird, ist es wenig verbreitet. Es gibt viele Techniker mit jahrelanger Erfahrung, denen noch nie ECC-RAM untergekommen ist.

Hinweis

Einige Speicherhersteller bezeichnen diese Technologie als *Error Checking and Correction*, die ebenfalls mit ECC abgekürzt wird. Lassen Sie sich von diesem Namen nicht aufs Glatteis führen, denn es handelt sich um dasselbe Verfahren. Es ist nur ein anderer Marketingdialekt für den Fehlerkorrekturcode.

Gepufferter oder registrierter Speicher

Bei der Beschaffung von Arbeitsspeicher, insbesondere von ECC-RAM, werden Sie früher oder später auf die Begriffe *registriertes* oder *gepuffertes RAM* stoßen. Bei diesen Speichermodulen gibt es ein zusätzliches Register, das als Puffer zwischen DIMM und Speicher-Controller fungiert. Diese zusätzliche Schaltung trägt elektronischen Problemen Rechnung, die bei Systemen mit sehr vielen Speichermodulen in Erscheinung treten können (z.B. Server).

Entscheidend ist hier, dass ein Mainboard entweder gepuffertes oder aber normales RAM (die typischen Speichermodule für Endkunden) verwendet, nicht aber beides. Wenn Sie ein Speichermodul des falschen Typs in das System einsetzen, das Sie aufrüsten, bleibt schlimmstenfalls der Bildschirm leer und Sie werden vermutlich herumrätseln, woran es liegt.

4.3 Der Umgang mit RAM

Wenn mich jemand fragt, welche einzelne Hardware-Anschaffung hinsichtlich der Leistungssteigerung eines Rechners am meisten bringt, dann sage ich immer dasselbe: »Erweitern Sie den Arbeitsspeicher.« RAM-Erweiterungen können die Gesamtleistung des Systems, die Verarbeitungsgeschwindigkeit und die Systemstabilität verbessern, sofern Sie dabei keine Fehler machen. Wenn Sie an dieser Stelle etwas vermasseln, dann kann das zu erheblichen Systeminstabilitäten und Abstürzen führen, die Neustarts erforderlich machen. Alle Techniker müssen wissen, wie sie den Arbeitsspeicher eines Rechners mit den verschiedenen RAM-Varianten erweitern können.

Damit eine Erweiterung des Arbeitsspeichers auch den gewünschten Erfolg hat, müssen Sie zunächst ermitteln, ob Arbeitsspeichermangel überhaupt die Ursache des Problems ist. Dann müssen Sie den für das System geeigneten Arbeitsspeicher auswählen (Bauform, Kapazität usw.). Und schließlich müssen Sie den Speicher noch ordnungsgemäß installieren. Bewahren Sie Speichermodule immer in antistatischer Verpackung auf, wenn sie nicht verwendet werden, und beachten Sie die Maßnahmen zur Vermeidung elektrostatischer Entladungen. Wie viele andere PC-Komponenten ist auch RAM *sehr* anfällig, was elektrostatische Entladungen und andere unsachgemäße Behandlungen betrifft (siehe Abbildung 4.20).

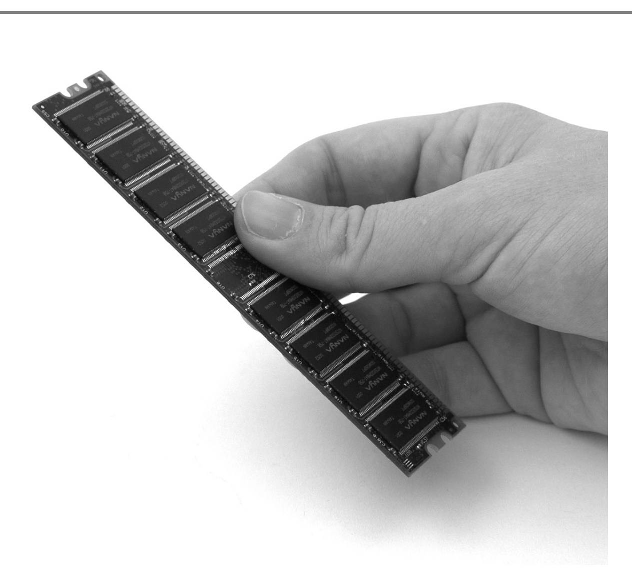


Abb. 4.20: Tun Sie das nicht! Die Kontakte zu berühren, ist keine gute Idee.

4.3.1 Ist mehr RAM erforderlich?

Zwei Symptome weisen darauf hin, dass mehr Arbeitsspeicher benötigt wird: allgemein langsame Reaktion des Systems und übermäßig häufige Festplattenzugriffe. Wenn der Start von Programmen ewig dauert und die Programme nur im Schneckentempo bzw. viel langsamer als gewünscht laufen, dann könnte mangelnder Arbeitsspeicher die Ursache sein.

Eine Freundin mit einem älteren Windows-System beschwerte sich bei mir darüber, dass der Rechner anfangs richtig schnell war, dass er jetzt aber die gewünschten Arbeiten, wie z.B. die Bildretusche mit Adobe Photoshop zu langsam verrichten würde. Im Laufe der Jahre hatten sich auf ihrem System mit nur 2 GB RAM neue Anwendungen und Aktualisierungen des Betriebssystems angesammelt, sodass es mit den zu erledigenden Aufgaben überfordert war. Der Arbeitsspeicher war ständig komplett ausgelastet, sodass das System unerträglich langsam wurde. Ich ersetzte ihr 2-GB-Speichermodul durch zwei 4-GB-Speichermodule und schon hatte sie das Kraftpaket, das sie sich gewünscht hatte.

Übermäßige Festplattenaktivitäten beim Wechsel zwischen Programmen weisen auf Arbeitsspeichermangel hin. Alle Rechner können bei knapp werdendem Arbeitsspeicher Teile der Festplatte als solchen nutzen.

Virtueller Speicher

Der Rechner verwendet einen Teil der Festplatte als Erweiterung des Arbeitsspeichers in Form des sogenannten *virtuellen Arbeitsspeichers*. Für den virtuellen Arbeitsspeicher wird ein Bereich auf der Festplatte oder einem SSD-Laufwerk für eine Auslagerungsdatei (*page file*, *swap file*) reserviert. Wenn dem Betriebssystem der echte Arbeitsspeicher ausgeht, weil zu viele Programme geladen wurden, dann lagert es wenig verwendete Programme aus dem Arbeitsspeicher aus, um den aktuell aktiven Programmen mehr Arbeitsspeicher zur Verfügung stellen zu können. Alle Versionen von Windows, macOS und Linux nutzen Auslagerungsdateien, weshalb wir uns nun am Beispiel eines Windows-PCs ansehen werden, wie diese funktionieren.

Wichtig

Die voreingestellte und empfohlene Größe der Auslagerungsdatei von Windows beträgt das Anderthalbfache der Größe des installierten RAMs.

Nehmen wir einmal an, dass der Rechner 4 GB Arbeitsspeicher besitzt. Abbildung 4.21 zeigt den Arbeitsspeicher des Systems in der Form eines Thermometers mit Unterteilungen zwischen 0 und 4 GB. Wenn weitere Programme (in der Abbildung A, B und C) geladen werden, wird mehr Arbeitsspeicher benötigt.

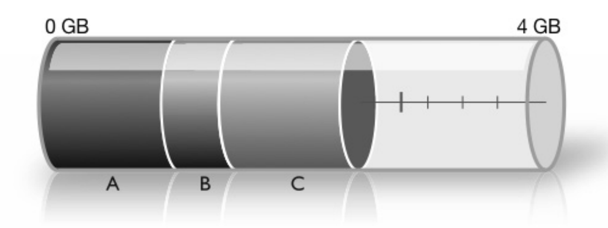


Abb. 4.21: Das »RAM-Thermometer« zeigt, wie Programme den Arbeitsspeicher belegen.

Ab einem gewissen Punkt ist nicht mehr genug RAM verfügbar, um weitere Programme laden zu können (siehe Abbildung 4.22). Natürlich könnten Sie nun einige Programme einfach beenden, um wieder mehr Platz für ein anderes Programm zu schaffen, aber Sie können eben nicht alle Programme gleichzeitig laufen lassen. An dieser Stelle kommt der virtuelle Speicher ins Spiel.

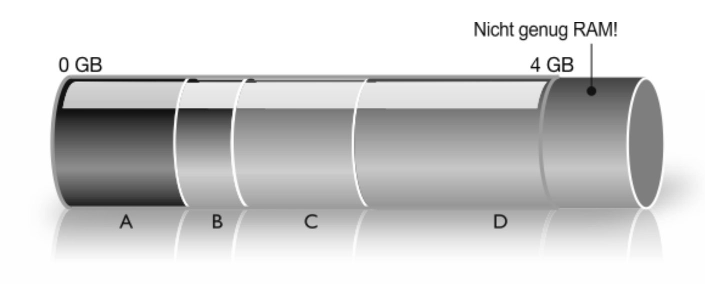


Abb. 4.22: Nicht genug RAM zum Laden des Programms D verfügbar

Windows sorgt für virtuellen Speicher, indem es eine Auslagerungsdatei anlegt, die sich irgendwo auf der Festplatte befindet. Die Auslagerungsdatei arbeitet wie ein temporärer Speicher. Windows nutzt die Auslagerungsdatei zu dem Zweck, laufende Programme zeitweise aus dem RAM entfernen zu können, damit andere Programme geladen und gestartet werden können. Sofern genug RAM für alle laufenden Programme verfügbar ist, benötigt Windows die Auslagerungsdatei nicht. Windows muss nur dann auf die Auslagerungsdatei zurückgreifen, wenn nicht genug RAM für alle laufenden Programme verfügbar ist.

Hinweis

Der virtuelle Speicher wird automatisch verwaltet und erfordert keinerlei Benutzereingriffe. Das gilt sowohl für Windows als auch für macOS und alle Linux-Distributionen.

Um gestartet werden zu können, benötigt das Programm D eine gewisse Mindestmenge RAM. Dies setzt voraus, dass ein anderes Programm (oder andere Programme) aus dem Arbeitsspeicher entfernt wird, ohne jedoch tatsächlich beendet zu werden. Windows überprüft alle laufenden Programme (in die-

sem Fall A, B und C) und entscheidet, welches dieser Programme am wenigsten gebraucht wird. Dieses Programm wird dann aus dem RAM entfernt bzw. ausgelagert und in die Auslagerungsdatei kopiert. Im Beispiel hat Windows das Programm B ausgewählt (Abbildung 4.23). Durch Entfernen des Programms B aus dem Arbeitsspeicher wird genug Platz zum Laden des Programms D frei (Abbildung 4.24).

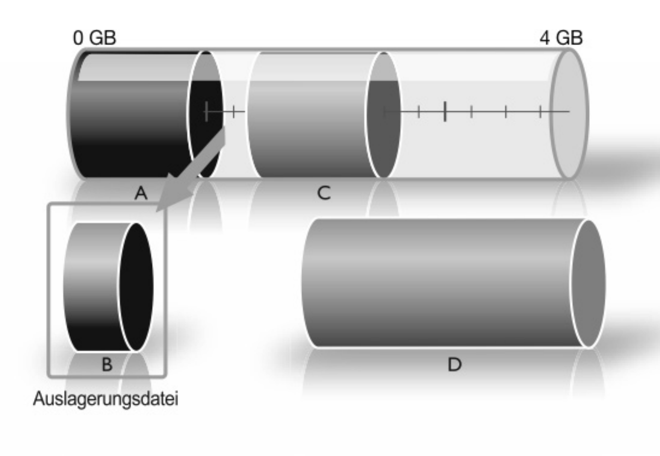


Abb. 4.23: Programm B wird aus dem Arbeitsspeicher entfernt.

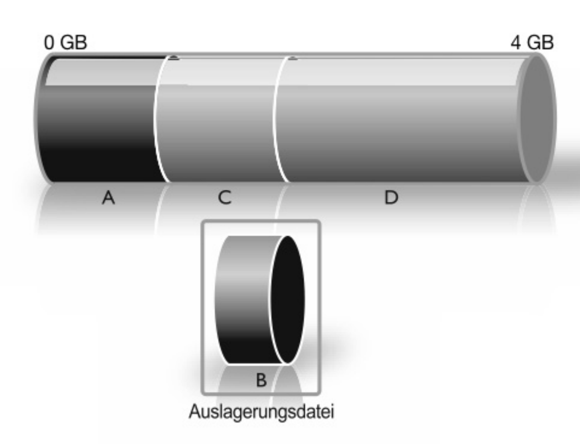


Abb. 4.24: Programm B wird in der Auslagerungsdatei abgelegt und schafft so Platz für Programm D.

Hier ist es wichtig zu verstehen, dass diese Aktivitäten unsichtbar im Hintergrund ablaufen. Das Fenster des Programms B wird immer noch zusammen mit allen anderen laufenden Programmen auf dem Bildschirm angezeigt! Der Benutzer erfährt nicht, dass sich das Programm B nicht mehr im Speicher befindet (Abbildung 4.25).

Was passiert dann aber, wenn Sie das Fenster von Programm B wieder anklicken, um es in den Vordergrund zu bringen? Das Programm kann nicht direkt aus der Auslagerungsdatei ausgeführt, sondern muss zurück in den Arbeitsspeicher geladen werden. Als Erstes trifft Windows jetzt eine Entscheidung darüber, welches Programm aus dem RAM entfernt werden muss; dieses Mal entscheidet es sich für Programm C (Abbildung 4.26). Anschließend lädt Windows Programm B wieder in den Arbeitsspeicher (Abbildung 4.27).

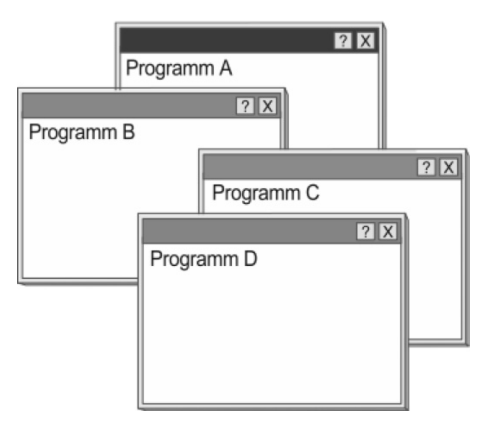


Abb. 4.25: Ob ein Programm ausgelagert wurde, ist ihm nicht anzusehen.

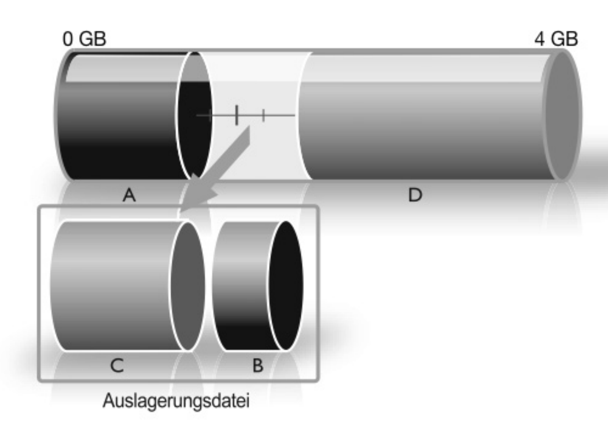


Abb. 4.26: Programm C wird ausgelagert.

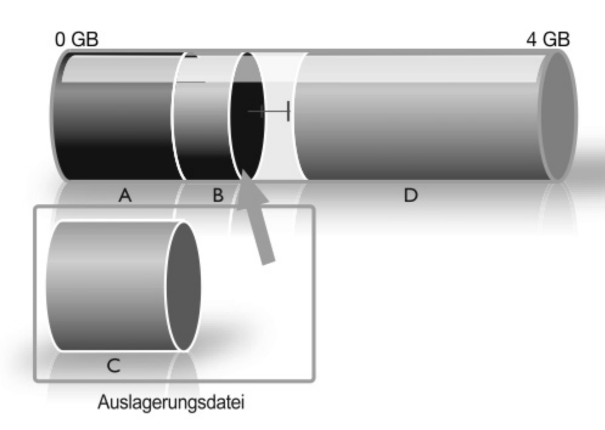


Abb. 4.27: Das Programm B wird wieder in den Arbeitsspeicher geladen.

Das Auslagern und das Zurückladen von Programmen kostet Zeit. Benutzer erhalten zwar keinen Hinweis darauf, dass Programme ausgelagert werden, jedoch wird der Rechner bei der Auslagerung deutlich langsamer. *Auslagerungsdateien* sind für den Betrieb von Windows überaus wichtig.

Windows erledigt das Auslagern automatisch. Gelegentlich treten aber Probleme auf, sodass die Größe der Auslagerungsdatei geändert oder diese gelöscht werden muss. Dann legt Windows die Auslagerungsdatei automatisch neu an. Der Name der Auslagerungsdatei lautet `PAGEFILE.SYS`. Man findet sie häufig im Stammverzeichnis des `C:`-Laufwerks, aber auch das kann geändert werden. Wo sie sich auch befindet, es handelt sich bei der Auslagerungsdatei um eine verborgene Systemdatei, was praktisch bedeutet, dass Sie die Ordneroptionen ändern müssen, wenn Sie die Datei sehen wollen.

Falls Windows zu häufig auf die Auslagerungsdatei zugreift, können Sie beobachten, dass die Festplatten-LED wild blinkt, wenn Windows ständig Programme zwischen Arbeitsspeicher und Auslagerungsdatei verschieben muss (*Disk-Thrashing*). Windows verwendet die Auslagerungsdatei zwar laufend, aber ständige und übermäßige Festplattenzugriffe weisen auf Arbeitsspeichermangel hin.

Empfehlungen für die Arbeitsspeicherkapazität

Microsoft gibt bei den verschiedenen Windows-Versionen für die minimale Speicherkapazität sehr niedrige Werte vor, um möglichst viele Anwender zur Aktualisierung oder zum Umstieg zu bewegen. Das ist auch gut so. Microsoft empfiehlt mindestens 1 GB RAM für 32-Bit-Versionen und 2 GB RAM für 64-Bit-Versionen von Windows. Dies gilt für alle Windows-Versionen. Meiner Ansicht nach führt das jedoch zu furchtbar lahmen Computern. Hier sind meine Empfehlungen:

- **32-Bit Windows**: 2 GB sind brauchbar, für gute Ergebnisse sollten es besser 4 GB sein.
- **64-Bit-Windows**: 4 GB sind brauchbar und 8 GB sind solide. Für anspruchsvollere, rechenintensive Aufgaben sollten es 16 GB oder mehr sein.

Für die neueste Version von macOS werden 2 GB RAM benötigt, aber wie Windows profitiert das reine 64-Bit-System deutlich von mehr RAM. Ich empfehle mindestens 4 GB, 8 GB für höhere Leistung oder mehr, um das System voll auszureizen.

Der minimale und der empfohlene Arbeitsspeicher für Linux hängen von der verwendeten Distribution ab. Bei den gebräuchlichsten Distros wie Ubuntu entsprechen sie denen von Windows und macOS. Viele Distros haben jedoch auch deutlich geringere Systemanforderungen.

Hinweis

Im Übrigen ist der Arbeitsspeicher bei manchen Geräten fest verlötet und kann nicht aufgerüstet werden. Dies gilt insbesondere für Smartphones und Tablets. Wenn Sie Geräte mit fest verbautem Arbeitsspeicher kaufen, sollten Sie bei der RAM-Ausstattung nicht geizen!

Ermittlung der aktuellen Arbeitsspeicherkapazität

Vor dem Kauf von Speichermodulen müssen Sie zunächst einmal wissen, wie viel Arbeitsspeicher sich bereits im Rechner befindet. Windows zeigt Ihnen die Arbeitsspeicherausstattung an, wenn Sie in der SYSTEMSTEUERUNG das Applet SYSTEM aufrufen (Abbildung 4.28). Sie können dieses Applet auch direkt über ein Tastenkürzel aufrufen und die Windows-Taste zusammen mit [Pause] betätigen.

Darüber hinaus gibt es noch die praktische Registerkarte LEISTUNG im Task-Manager (Abbildung 4.29). Sie enthält viele Informationen über die Nutzung des Arbeitsspeichers Ihres PCs Drücken Sie die Tastenkombination [Strg] + [⇧] + [ESC], um den Task-Manager aufzurufen und wählen Sie die Registerkarte LEISTUNG.

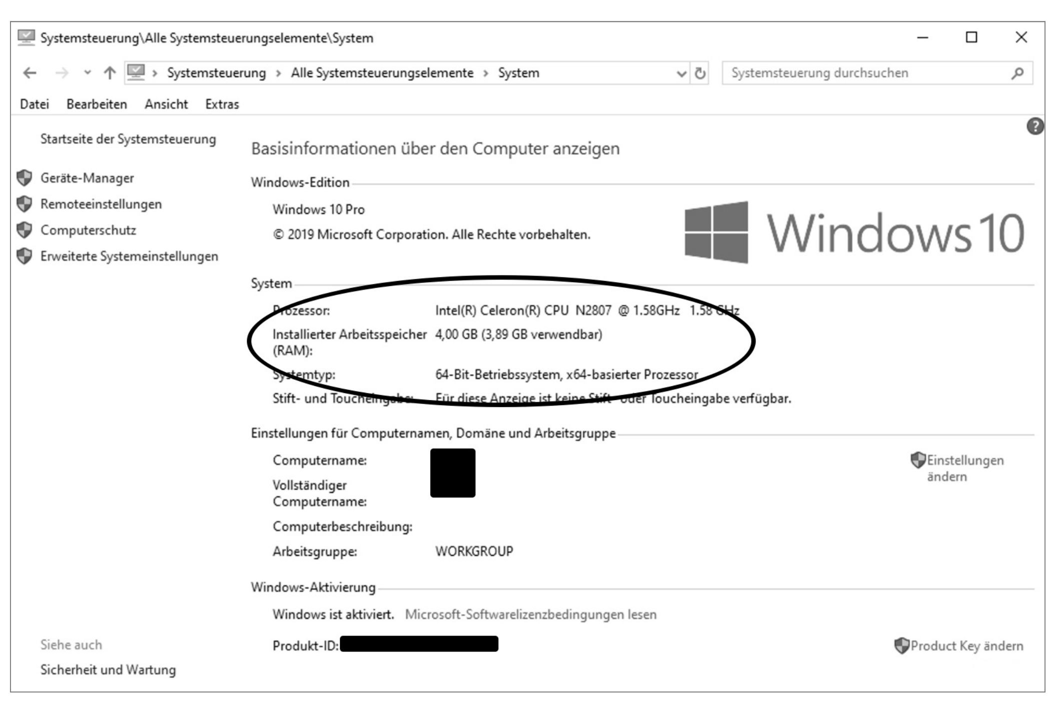


Abb. 4.28: Dieses System verfügt nur über 4 GB Arbeitsspeicher.

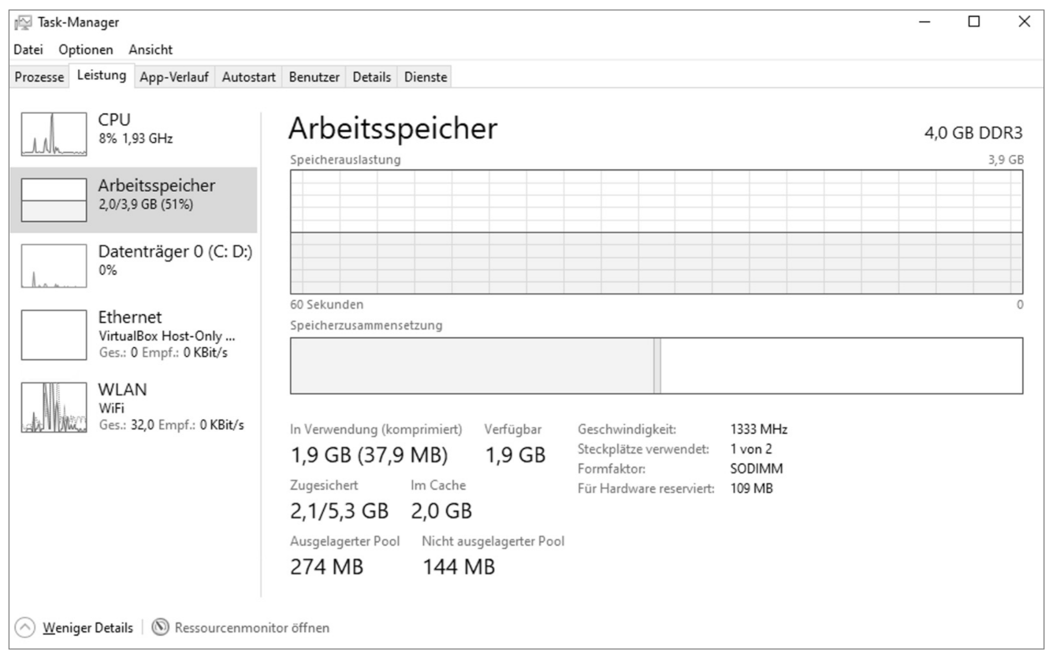


Abb. 4.29: Die Registerkarte LEISTUNG im Task-Manager von Windows 10

ReadyBoost

Herkömmliche (rotierende) Festplatten bieten bei der Verwendung als virtueller Arbeitsspeicher keine besonders gute Leistung. In Windows gibt es eine Funktion namens *ReadyBoost*, die es ermöglicht, Flash-Speichergeräte, wie etwa USB-RAM-Sticks oder Speicherkarten, als extrem schnellen, eigens für diesen Zweck bereitgestellten virtuellen Speicher zu verwenden. Der Geschwindigkeitszuwachs durch ReadyBoost gegenüber der Nutzung einer herkömmlichen Festplatte kann beträchtlich sein, denn die Schreib/Lesegeschwindigkeit von Flash-Speicher lässt normale Festplatten alt aussehen.

Wenn Sie ein für ReadyBoost geeignetes Gerät installiert oder angeschlossen haben (z.B. eine Speicherkarte oder einen USB-RAM-Stick), klicken Sie unter COMPUTER mit der rechten Maustaste auf das Gerät und wählen Sie im Kontextmenü EIGENSCHAFTEN. Klicken Sie auf die Registerkarte READYBOOST und wählen Sie entweder DIESES GERÄT FÜR READYBOOST RESERVIEREN oder DIESES GERÄT VERWENDEN (Abbildung 4.30). Klicken Sie dann auf ÜBERNEHMEN, um Ihr System zu beschleunigen.

Hinweis

ReadyBoost ist nicht für alle Systeme geeignet. Ein modernes System mit SSD-Laufwerk wird kaum einen Nutzen daraus ziehen. Das Hinzufügen von mehr Arbeitsspeicher bringt einen größeren Geschwindigkeitsschub, als mit ReadyBoost herumzubasteln. Fügen Sie Arbeitsspeicher hinzu und lassen Sie lieber die Finger von ReadyBoost. Sie brauchen es nur für die Prüfungen zu kennen.



Abb. 4.30: Reservieren eines Flash-Laufwerks für ReadyBoost zur Beschleunigung des Systems

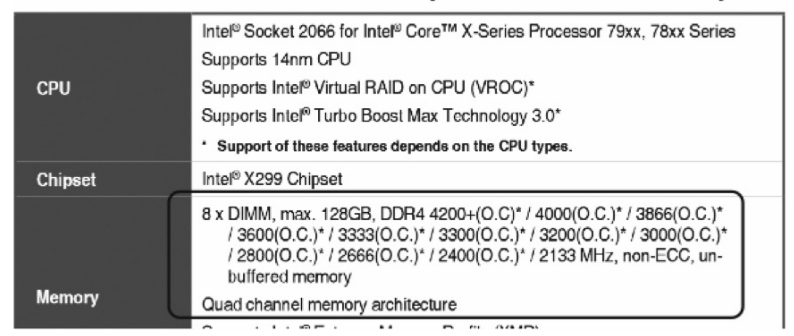
4.3.2 Beschaffung der richtigen Speichermodule

Für die perfekte Aufrüstung des Arbeitsspeichers bestimmen Sie die zu installierende optimale Speichermenge und beschaffen dann die zum Mainboard passenden Speichermodule. Die ersten beiden Schritte zur Erreichung dieses Ziels bestehen im Öffnen des Rechnergehäuses und einem Blick in das

Mainboard-Handbuch. Öffnen Sie das Gehäuse und sehen Sie nach, wie viele RAM-Module dort bereits installiert sind und wie viele Speichersteckplätze noch frei sind.

Werfen Sie dann einen Blick in das Mainboard-Handbuch oder auf die Website des Herstellers, um festzustellen, welche Speicherkapazität vom System maximal unterstützt wird und welche Speichertechnologie sich für das System eignet.

Sie können in einem System, das nur DDR3-SDRAM unterstützt, keine DDR4-Module verwenden und letztlich ist es wenig sinnvoll, in ein System, das maximal 4 GB Arbeitsspeicher unterstützt, zwei 4-GB-DIMMs einzubauen! Abbildung 4.31 zeigt die Grenzen der Arbeitsspeicherkapazität für ein ASUS-Mainboard.



ROG RAMPAGE VI EXTREME specifications summary

CPU	Intel® Socket 2066 for Intel® Core™ X-Series Processor 79xx, 78xx Series Supports 14nm CPU Supports Intel® Virtual RAID on CPU (VROC)* Supports Intel® Turbo Boost Max Technology 3.0* * Support of these features depends on the CPU types.
Chipset	Intel® X299 Chipset
Memory	8 x DIMM, max. 128GB, DDR4 4200+(O.C)* / 4000(O.C.)* / 3866(O.C.)* / 3600(O.C.)* / 3333(O.C.)* / 3300(O.C.)* / 3200(O.C.)* / 3000(O.C.)* / 2800(O.C.)* / 2666(O.C.)* / 2400(O.C.)* / 2133 MHz, non-ECC, unbuffered memory Quad channel memory architecture

Abb. 4.31: Das Mainboard-Handbuch gibt an, wie viel RAM ein Mainboard verwalten kann.

Hinweis

Das Freeware-Programm *CPU-Z* teilt Ihnen mit, wie viele Speichersteckplätze es auf Ihrem Mainboard gibt, wie viele davon in Verwendung sind und welche Art von Speicher sich darin befindet. Höchst praktisch! CPU-Z kann nicht nur die Latenz der Speichermodule ermitteln, sondern diese auch noch für unterschiedliche Mainboard-Geschwindigkeiten angeben. Probieren Sie das Programm doch einfach einmal aus. Sie können es unter `www.cpuid.com` herunterladen.

Mischen auf eigene Gefahr

Alle Mainboards unterstützen Module unterschiedlicher Kapazität. Wenn Sie drei Steckplätze haben, können Sie ein 2-GB-Modul in einem und ein 4-GB-Modul in einem anderen installieren und werden damit sehr wahrscheinlich Erfolg haben. Um für maximale Systemstabilität zu sorgen, sollten Sie jedoch möglichst einheitliche Speichermodule verwenden. Wählen Sie Speichermodule aus, deren technische Daten, Kapazität und Geschwindigkeit übereinstimmen.

Mischen unterschiedlicher Geschwindigkeiten

Angesichts so vieler unterschiedlicher DRAM-Geschwindigkeiten kommen Sie möglicherweise hier und da in Versuchung, DRAM-Typen unterschiedlicher Geschwindigkeiten in ein und demselben System gemischt einzusetzen. Meist funktioniert das auch, sofern die Module nur durchweg schnell genug sind. Sie sind jedenfalls auf der sicheren Seite, wenn Sie diese einfache Regel befolgen: Verwenden Sie immer die im Mainboard-Handbuch angegebene DRAM-Geschwindigkeit und stellen Sie sicher, dass alle einzelnen Module diese Geschwindigkeit auch tatsächlich unterstützen. Das Mischen verschiedener DRAM-Geschwindigkeiten kann schlimmstenfalls alle paar Minuten oder gar Sekunden zu Systemabstürzen und damit möglicherweise auch zu Datenverlust führen. Der Einsatz unterschiedlich schneller Module kann funktionieren. Sie sollten aber Ihre Steuererklärung nicht gerade an einem solchen System erledigen und das System erst einmal ein paar Tage lang wirklich sorgfältig testen, bis Sie

zuverlässig wissen, dass es stabil arbeitet. Kaputtmachen können Sie während der Experimentierphase nichts – außer vielleicht ein paar Daten.

Genug gewarnt! Moderne Mainboards bieten hinsichtlich des Mischens von RAM-Geschwindigkeiten eine gewisse Flexibilität. Erstens können Sie Module verwenden, deren Geschwindigkeit über den Vorgaben des Mainboards liegt. Falls das System z.B. PC19200 DDR4-RAM benötigt, können Sie normalerweise auch PC25600 DDR4-RAM verwenden, ohne dass Probleme auftreten. Schnellere Module allein machen das System allerdings nicht schneller – versprechen Sie sich davon also keine Leistungssteigerung.

Zweitens lassen sich – wie bereits erwähnt – meist Module einer Geschwindigkeit in einer Bank und Module einer anderen Geschwindigkeit in einer zweiten Bank einbauen, sofern beide Geschwindigkeiten mindestens den Vorgaben des Mainboards genügen. Versuchen Sie aber keinesfalls bei einem Mainboard, das mit Zweikanal-DDR arbeitet, DRAM-Module unterschiedlicher Geschwindigkeit in dieselbe Bank einzubauen.

4.3.3 DIMMs installieren

Die Installation von DRAM ist so einfach, dass es sich dabei um eine der wenigen Arbeiten handelt, die ich sogar Nicht-Technikern empfehle. Zuerst legen Sie ein Antistatikarmband an oder berühren Metall am Netzteil, um sich zu erden und elektrostatische Entladungen zu verhindern. Anschließend klappen Sie die Seitenhalterungen an den RAM-Steckplätzen von ihrer aufrechten Position aus nach unten. Nehmen Sie ein RAM-Modul, ohne dabei dessen Kontakte zu berühren! Richten Sie das Modul dann so aus, dass die Positionen der Aussparungen mit den Positionen der Nasen im Speichersteckplatz übereinstimmen (Abbildung 4.32). Drücken Sie das Modul dann senkrecht und entschlossen in den Sockel, bis es festsitzt. Achten Sie darauf, dass die Platine richtig einrastet. Sie werden bemerken, dass die beiden Seitenhalterungen nach innen in die Aussparungen der Module greifen und ebenfalls einrasten, wenn die Speichermodule richtig sitzen.



Abb. 4.32: Ein Speichermodul installieren

Wenn Sie die richtigen Speichermodule für das System ausgewählt haben, dann sollte Ihr Mainboard installierte DIMMs erkennen und sich automatisch passend konfigurieren. RAM-Hersteller haben moderne Speichermodule mit einem nützlichen Chip versehen, dem sogenannten *SPD-Chip* (*Serial*

Presence Detect, Abbildung 4.33). Im SPD-Chip sind alle Informationen über ein DRAM-Modul gespeichert, wie neben anderen technischen Daten z.B. auch Kapazität, Geschwindigkeit und Art (ECC-, Register-DRAM oder nicht).

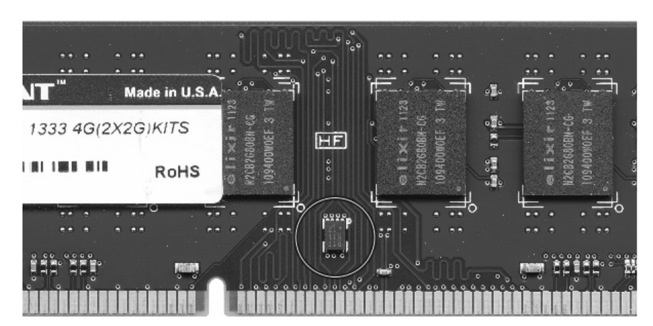


Abb. 4.33: SPD-Chip auf einem Speichermodul

Wenn ein PC bootet, fragt er den SPD-Chip ab, sodass der MCC weiß, wie viel RAM sich auf dem Modul befindet, wie schnell es ist, und verschiedene andere Informationen. Der SPD-Chip kann von jedem Programm abgefragt werden. Abbildung 4.34 zeigt, wie das Programm CPU-Z die Informationen aus dem SPD darstellt.

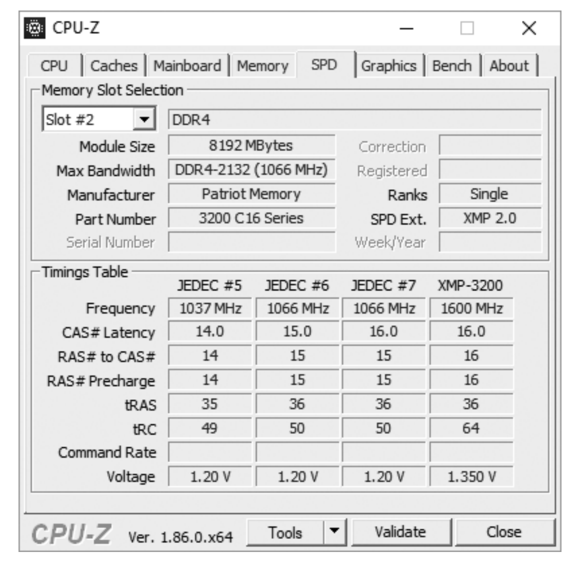


Abb. 4.34: CPU-Z mit Informationen zu einem Speichermodul

Alle neuen Systeme verlassen sich auf den SPD-Chip, um die RAM-Timings für ein System beim Booten genau einzustellen. Wenn Sie ein Speichermodul mit fehlerhaftem SPD-Chip einsetzen, erhalten Sie eine POST-Fehlermeldung (*Power-On Self Test*), und das System bootet nicht. Defekte SPD-Chips lassen sich nicht reparieren. Sie müssen ein neues Speichermodul kaufen.

4.3.4 Einbau von SO-DIMMS in Laptops

Vor nicht allzu langer Zeit waren Speichererweiterungen bei Laptops entweder nahezu unmöglich oder man musste dazu das Gerät zum Hersteller einsenden. Lange benutzten alle Laptop-Hersteller

eigene Speichermodule, die schwierig zu installieren und überaus teuer waren. Mit der Verbreitung der SO-DIMMs wurde dieses Problem für eine Weile gelöst – bis in extrem flachen Laptops fest verlöteter Arbeitsspeicher verbaut wurde. Bei den meisten größeren Laptops sind die SO-DIMMs aber auch heute noch relativ leicht zugänglich, sodass der Austausch oder die Erweiterung der Speichermodule einfach ist.

Um an die Module zu gelangen, müssen Sie meist eine Abdeckung entfernen oder die Tastatur abheben. Die genaue Vorgehensweise hängt vom jeweiligen Hersteller des Laptops ab. Abbildung 4.35 zeigt eine typische Klappe, hinter der sich die Speichersteckplätze eines Laptops befinden. Sie können die Abdeckung wegschieben, um an die SO-DIMMs zu kommen. Bringen Sie die Kontaktleiste in Position und drücken Sie das SO-DIMM dann in den Sockel hinein, bis die Haltevorrichtung einrastet (Abbildung 4.36).

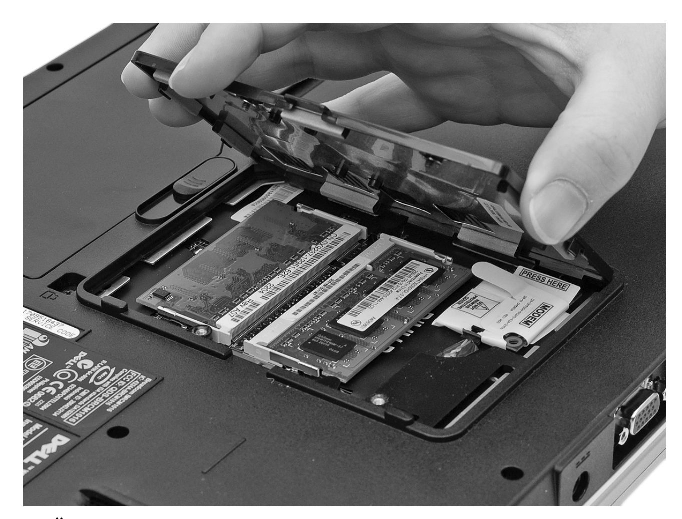


Abb. 4.35: Über eine Klappe auf der Unterseite des Laptops ist der Speicher zugänglich.



Abb. 4.36: Einsetzen eines SO-DIMMs

Bevor Sie irgendwelche Arbeiten am Laptop vornehmen, schalten Sie das System aus, trennen es von der Steckdose und entfernen den Akku (sofern das möglich ist). Und verwenden Sie ein Antistatikarmband, denn Laptops reagieren auf antistatische Entladungen noch empfindlicher als Desktop-PCs.

4.4 Fehlerbehebung beim Arbeitsspeicher

Speicherfehler zeigen sich in modernen Systemen auf verschiedene Art und Weise. Dabei kann es sich um Systemabstürze, Seitenfehler und andere Fehlermeldungen handeln. Diese Fehler können auf defektes RAM hinweisen, haben aber häufig auch andere Ursachen, die mit dem Arbeitsspeicher absolut nichts zu tun haben. Dies gilt insbesondere für unregelmäßig und scheinbar zufällig auftretende Probleme. Techniker müssen solche Fehler erkennen und feststellen können, welche Systemkomponenten den Speicherfehler verursachen.

Manche Systemabstürze und Seitenfehler (die häufig gemeinsam auftreten) unter Windows können auf Speicherprobleme hindeuten. Ein Systemabsturz liegt dann vor, wenn der Computer nicht mehr funktioniert. Bei einem Seitenfehler handelt es sich um einen weniger ernsten Fehler, der durch Speicherprobleme entstehen kann, aber nicht unbedingt auf Probleme mit dem System-RAM hinweist. Gewisse Seitenfehler sehen aber nur wie Speicherfehler aus, da Windows in solchen Fällen beängstigende Fehlermeldungen mit hexadezimalen Ziffernfolgen wie z.B. »KRNL386 verursachte einen Seitenfehler unter der Speicheradresse 03F2:25A003BC« anzeigt. Nur weil die Fehlermeldung auf eine Speicheradresse verweist, muss es sich aber noch lange nicht um ein Speicherproblem handeln. Notieren Sie sich die Speicheradresse. Sollte sie in späteren Fehlermeldungen erneut auftauchen, ist sehr wahrscheinlich ein Speichermodul defekt. Zeigt Windows dagegen unterschiedliche Speicheradressen an, dann sollten Sie den Schuldigen an anderer Stelle vermuten.

Vereinzelt kann es im PC immer zu katastrophalen Ereignissen kommen, wenn irgendein kleines Elektron den großen roten Panikschalter betätigt und das Betriebssystem bestimmte Funktionen sperren muss, um Daten zu schützen. Dieser Panikschalter im PC wird *NMI* (*Non-Maskable Interrupt* – Nicht maskierbarer Interrupt) genannt. Dabei handelt es sich einfach um eine Unterbrechung, die von der CPU nicht ignoriert werden kann. Dem Anwender präsentiert sich ein NMI in Form des *proprietären Absturzbildschirms*. Unter Windows 7 handelt es sich dabei z.B. um die von Technikern als *Blue Screen* (Blue Screen *of Death* (BSoD)) bezeichnete Bildschirmanzeige – ein leuchtend blauer Bildschirm, auf dem eine bedrohlich klingende Fehlermeldung angezeigt wird (Abbildung 4.37).



Abb. 4.37: Proprietärer Absturzbildschirm

Windows 8/8.1/10 zeigen einen Blue Screen mit einem traurigen Gesicht und einem Text, der aussagt, dass Windows ein Problem hat. Starten Sie den Computer in diesem Fall neu. macOS zeigt ein sich drehendes regenbogenfarbiges Scheibchen, das als *Pinwheel of Death* (Windrädchen des Todes) oder scherzhaft auch als *Spinning Pizza of Death* (rotierende Pizza des Todes) bezeichnet wird, oder startet den Computer einfach neu.

Sicherlich können defekte Speicherbausteine einen NMI auslösen. Beim Schuldigen handelt es sich aber oft um Fehler in Programmen oder Codekonflikte. Der Blue Screen sieht unter den verschiedenen Betriebssystemen unterschiedlich aus und es wären ausführliche Erläuterungen erforderlich, um alle denkbaren Variationen zu beschreiben, für die hier einfach kein Platz ist. Daher will ich mich an dieser Stelle auf die Aussage beschränken, dass der Arbeitsspeicher die Ursache des Problems sein *kann*, das zur Anzeige des hübschen blauen Bildschirms oder des Pinwheels geführt hat.

Periodisch auftretende Speicherfehler können schließlich die verschiedensten Ursachen wie beispielsweise ein defektes Netzteil, Schwankungen der Stromversorgung, Programmfehler, Hardwarefehler usw. haben. Fehler dieser Art zeigen sich in der Form von Abstürzen, allgemeinen Schutzverletzungen und Seitenfehlern, verweisen aber höchst selten auf dieselbe Adresse und treten üblicherweise bei verschiedenen Anwendungen auf. Prüfen Sie bei sporadisch auftretenden Fehlern, die nicht bestimmten Anwendungen zugeordnet werden können, immer zunächst das Netzteil.

Sobald Sie ein mögliches Speicherproblem diagnostiziert haben, verfügen Sie über eine Reihe von Testmöglichkeiten. Erstens bieten verschiedene Unternehmen RAM-Testgeräte an. Zweitens können Sie so wie ich nach der Methode »Austauschen und Hoffen« verfahren. Öffnen Sie dazu das Systemgehäuse und ersetzen Sie jeweils ein Modul durch ein anderes, von dem Sie wissen, dass es ordnungsgemäß funktioniert (vielleicht haben Sie noch eines herumliegen?). Diese Methode ist zwar ziemlich zeitaufwendig, funktioniert aber zuverlässig. Bei den heutigen PC-Preisen würde jedenfalls der Austausch des kompletten Rechnersystems weniger als ein spezielles RAM-Testgerät kosten.

Drittens könnten Sie auch *Speichertestprogramme* ausführen. Da die Testprogramme in den zu prüfenden Speicher geladen werden müssen, besteht immer eine geringe Wahrscheinlichkeit, dass allein durch das Ausführen der Testsoftware Fehler verursacht werden. Es gibt einige sehr gute kostenlose Testprogramme. Windows 7 und neuere Windows-Versionen bringen das *Speicherdiagnosetool* mit, das automatisch Ihren Arbeitsspeicher untersuchen kann, wenn es Probleme gibt. Falls Sie ein anderes Betriebssystem verwenden: Mein Favorit ist das Open-Source-Programm *Memtest86+* (`www.memtest86.com`). Memtest86+ überprüft Ihren Arbeitsspeicher eingehend und meldet gegebenenfalls fehlerhaften Speicher (Abbildung 4.38).

```
      Memtest86  v4.10        | Pass 11% ####
Athlon 64 X2 2210 MHz         | Test 84% ################################
L1 Cache:   64K  17266 MB/s   | Test #4  [Moving inversions, random pattern]
L2 Cache:  512K   4316 MB/s   | Testing:  184K - 2048M 4095M
L3 Cache:        None         | Pattern:   8ce395a0
Memory  : 4095M   2840 MB/s   |------------------------------------------
Chipset : AMD K8 IMC (ECC : Disabled)
Settings: RAM : 442 MHz (DDR884) / CAS : 5-5-5-18 / DDR2 (128 bits)

 WallTime   Cached  RsvdMem   MemMap   Cache  ECC  Test  Pass  Errors ECC Errs
 ---------  ------  -------  --------  -----  ---  ----  ----  ------ --------
   0:04:38   4095M      12K    e820      on   off   Std     0      27        0
 ---------------------------------------------------------------------------
Tst  Pass   Failing Address           Good      Bad      Err-Bits  Count Chan
---  ----  -----------------------  --------  --------  --------  ----- ----
  4     0  00050ff4824 -  1295.9MB  277aa3d4  2f7aa3d4  08000000     19
  4     0  000507f0824 -  1287.9MB  277aa3d4  2f7aa3d4  08000000     20
  4     0  000101e4824 -   257.8MB  277aa3d4  2f7aa3d4  08000000     21
  4     0  00050ff4824 -  1295.9MB  277aa3d4  2f7aa3d4  08000000     22
  4     0  000101e4824 -   257.8MB  277aa3d4  2f7aa3d4  08000000     23
  4     0  0001007c824 -   256.4MB  277aa3d4  2f7aa3d4  08000000     24
  4     0  0007007f824 -  1792.4MB  127a0592  327a0592  20000000     25
  4     0  000507f0824 -  1287.9MB  864310cc  8e4310cc  08000000     26
  4     0  00050ff4824 -  1295.9MB  864310cc  8e4310cc  08000000     27
(ESC)Reboot  (c)configuration  (SP)scroll_lock  (CR)scroll_unlock
```

Abb. 4.38: Memtest86+ bei der Arbeit

Hinweis

Die *allgemeine Schutzverletzung* (*GPF – General Protection Fault*) ist ein Fehler, der zum Absturz einer Anwendung führen kann. Häufig werden sie aber durch Programme verursacht, die sich gegenseitig auf die Füße treten. Kapitel 16, *Fehlerbehebung*, beschäftigt sich eingehender mit GPFs und anderen Windows-Fehlern.

4.5 Wiederholung

4.5.1 Fragen

1. Stefan baut ein zweites, 288-poliges DIMM mit 8 GB Kapazität in seinen PC ein, womit er die Arbeitsspeicherkapazität auf insgesamt 16 GB erhöhen will. Der PC enthält einen Intel Core i7-Prozessor mit 3 GHz und hat vier 288-polige DIMM-Steckplätze auf dem Mainboard. Wenn Stefan den PC einschaltet, zeigt die Einstellungen-App jedoch nur 8 GB RAM an. Welches Problem ist am wahrscheinlichsten?
   A. Stefan hat das RAM nicht korrekt eingebaut.
   B. Stefan hat DDR4-RAM in einen DDR3-Steckplatz eingebaut.
   C. Die CPU weiß mit 16 GB RAM nichts anzufangen.
   D. Das Mainboard kann jeweils nur einen RAM-Steckplatz verwenden.
2. Alex will 8 GB PC1280-DDR3-RAM in einen zwar betagten, aber immer noch gut funktionierenden Desktop-Computer einbauen. Das System besitzt ein 200-MHz-Mainboard und momentan 4 GB Nicht-ECC-SDRAM. Was sollte Alex vor der Installation noch wissen?
   A. Welche RAM-Geschwindigkeit er benötigt.
   B. Welchen RAM-Typ er benötigt.
   C. Wie viele Pins das RAM besitzt.
   D. Ob das System mit so viel Arbeitsspeicher umgehen kann.
3. Was ist der wichtigste Grund dafür, dass DDR4-RAM schneller als DDR3-RAM ist?
   A. Die Kerngeschwindigkeit der DDR4-RAM-Chips ist schneller.
   B. Die E/A-Geschwindigkeit des DDR4-RAMs ist schneller.
   C. DDR3 ist Dual-Channel-, DDR4 ist Quad-Channel-RAM.
   D. DDR3-RAM verwendet 240-polige, DDR4 288-polige DIMMs.
4. Welchen Begriff benutzt man für die verzögerte Reaktion des Arbeitsspeichers auf Anforderungen des MCCs?
   A. Varianz
   B. MCC-Lücke
   C. Latenz
   D. Abrufintervall
5. Wie zeigt Windows einen NMI an?
   A. Blue Screen of Death
   B. Pinwheel of Death
   C. Interrupt of Death
   D. NMIs kommen nur auf macOS-Systemen vor

6. Felix hat ein neues Mainboard für einen AMD-Prozessor gekauft. Er hat zwei der drei Speichersteckplätze mit zwei DDR3-Modulen bestückt und damit insgesamt 8 GB Arbeitsspeicher. Wenn er CPU-Z ausführt, um das System zu testen, meldet die Software, dass es sich um Single-Channel-Speicher handelt. Was könnte die Ursache für das Problem sein? (Wählen Sie die beste Antwort aus.)
   A. Sein Mainboard unterstützt nur Single-Channel-Speicher.
   B. Sein Mainboard unterstützt Dual-Channel-Speicher nur für DDR2-RAM, nicht für DDR3.
   C. Er muss ein drittes RAM-Modul installieren, um den Dual-Channel-Speicher zu aktivieren.
   D. Er muss eines der installierten Module in einen anderen Steckplatz stecken, um den Dual-Channel-Speicher zu aktivieren.
7. Welches der folgenden Applets der Systemsteuerung zeigt die Menge des installierten Arbeitsspeichers an?
   A. System
   B. Geräte und Drucker
   C. Geräte-Manager
   D. Wartungscenter
8. Wie ermitteln Sie am besten die maximale Gesamtspeicherkapazität und den RAM-Typ, der von Ihrem System benötigt wird?
   A. Sie lesen im Mainboard-Handbuch nach.
   B. Sie öffnen das Gehäuse und sehen sich die Speichermodule an.
   C. Sie sehen im Geräte-Manager nach.
   D. Sie probieren es mit dem Applet SYSTEM in der Systemsteuerung.
9. Sebastian hat ein drittes, funktionierendes Speichermodul in seinen Core-i7-Rechner eingebaut, der nun insgesamt über 12 GB RAM verfügt. Nach ein paar Tagen treten plötzlich zufällige Systemabstürze und Neustarts auf, insbesondere bei speicherintensiven Aufgaben und Spielen. Welche Ursache hat das Problem am wahrscheinlichsten?
   A. Sebastian hat DDR2-RAM in einem DDR3-System installiert.
   B. Sebastian hat DDR3-RAM in einem DDR4-System installiert.
   C. Sebastian hat Speichermodule installiert, deren Geschwindigkeit oder Eigenschaften nicht den Systemanforderungen entsprechen.
   D. Sebastian hat ein Speichermodul installiert, das schneller als der bisherige Arbeitsspeicher des Systems ist.
10. Lena hat ein zweites DDR4-Speichermodul in ihrem Core-i5-System installiert, womit das System nun insgesamt über 16 GB Arbeitsspeicher verfügt. Nach kurzer Zeit treten jedoch Blue Screens auf. Was könnte die Ursache sein?
    A. Sie hat fehlerhafte Speichermodule eingebaut.
    B. Das Mainboard kann nur 12 GB RAM verwalten.
    C. Das Mainboard benötigt Dual-Channel-RAM.
    D. Es gibt kein Problem. Windows macht das anfangs immer, aber nach ein paar Abstürzen wird es besser.

4.5.2 Antworten

1. **A.** Wahrscheinlich sitzt das Speichermodul nicht richtig.
2. **D.** Alex muss prüfen, ob das System so viel RAM verwalten kann.
3. **B.** Die E/A-Geschwindigkeit von DDR4-RAM ist höher als diejenige von DDR3-RAM (obwohl die Latenz höher ist).

4. **C.** Latenz ist der Begriff für die verzögerte Reaktion des Speichers auf Anforderungen des MCCs.
5. **B.** Ein nicht maskierbarer Interrupt wird von Windows als Blue Screen of Death angezeigt.
6. **D.** Möglicherweise müssen die Speichermodule beim verwendeten Mainboard in bestimmten Steckplätzen installiert werden, damit der Dual-Channel-Betrieb funktioniert. Dann sollte Felix eines der installierten Module in einen anderen Steckplatz einbauen, um den Dual-Channel-Betrieb zu aktivieren. (Außerdem sollte er im Handbuch für das Mainboard nachlesen, welches die richtigen Steckplätze sind.)
7. **A.** Verwenden Sie das Applet SYSTEM, um die Menge des installierten Arbeitsspeichers anzuzeigen.
8. **A.** Am besten ermittelt man die Gesamtspeicherkapazität und die für ein System zu verwendende Art der Speichermodule mithilfe des Mainboard-Handbuchs.
9. **C.** Sehr wahrscheinlich hat Sebastian Speicher installiert, dessen Geschwindigkeit und Eigenschaften nicht mit den bereits installierten Modulen übereinstimmen.
10. **A.** Wenn ein System fehlerfrei lief, nach der Installation neuer Komponenten aber Probleme auftreten, ist es sehr wahrscheinlich, dass eine der neuen Komponenten fehlerhaft ist.

BIOS und CMOS | 5

Themen in diesem Kapitel:

- Die Aufgaben des BIOS
- Optionen des CMOS-Setup-Programms
- ROM und Gerätetreiber
- Fehlersuche beim Selbsttest (POST – Power-On Self-Test)
- Wartung von BIOS und CMOS

In Kapitel 3, *Mikroprozessoren*, haben Sie erfahren, wie Adressbus und externer Datenbus den Arbeitsspeicher über den MCC (Memory Controller Chip, dt. Speicher-Controller-Chip) so mit der CPU verbinden, dass Programme ausgeführt und Daten übertragen werden können. Sofern die Komponenten ordnungsgemäß mit Strom versorgt werden, läuft der Rechner schon. Allerdings würden Sie sich mit diesem Gerät wohl zu Tode langweilen, da es keine Möglichkeit gibt, ihn praktisch zu nutzen! Ein PC braucht Geräte wie Tastatur und Maus, um Eingaben entgegennehmen zu können, und Ausgabegeräte wie Bildschirm und Lautsprecher, um den Benutzer über den aktuellen Status der aktiven Programme zu informieren. Und es werden auch Geräte benötigt, mit denen Daten dauerhaft auch nach dem Abschalten des Rechners gespeichert werden können, wie z.B. SSD-Laufwerke.

In diesem Kapitel werden ausführlich die Komponenten vorgestellt, die die Kernfunktionen eines PCs steuern. Zunächst beschäftigen wir uns in einigen Abschnitten damit, wie und warum das Ganze funktioniert. Danach betrachten wir die Hardware und deren Selbsttests. Das Kapitel endet mit Erläuterungen dazu, was bei der Wartung der grundlegenden Systemkomponenten zu beachten ist.

1001

5.1 Wir müssen miteinander reden

Damit die CPU eine Tastatur oder eine Festplatte verwenden kann, müssen sie über eine physische Verbindung miteinander kommunizieren. Darüber hinaus können solche Peripheriegeräte (für gewöhnlich) nicht direkt mit der CPU kommunizieren. Zur Kommunikation benötigt man einen Controller-Chip, der das Gerät mit der CPU verbindet (Abbildung 5.1).



Abb. 5.1: Ein Controller-Chip fungiert als Schnittstelle.

Damit die CPU mit einem Gerät kommunizieren kann, benötigt man zuerst irgendeine Art der Verbindung – einen Kommunikationsbus, der es der CPU ermöglicht, Befehle an die Geräte zu senden und von diesen entgegenzunehmen. Um diese Verbindung herzustellen, erweitern wir den Datenbus

und den Adressbus, damit sie als Verbindung zwischen der CPU und den Controllern im PC dienen (Abbildung 5.2).

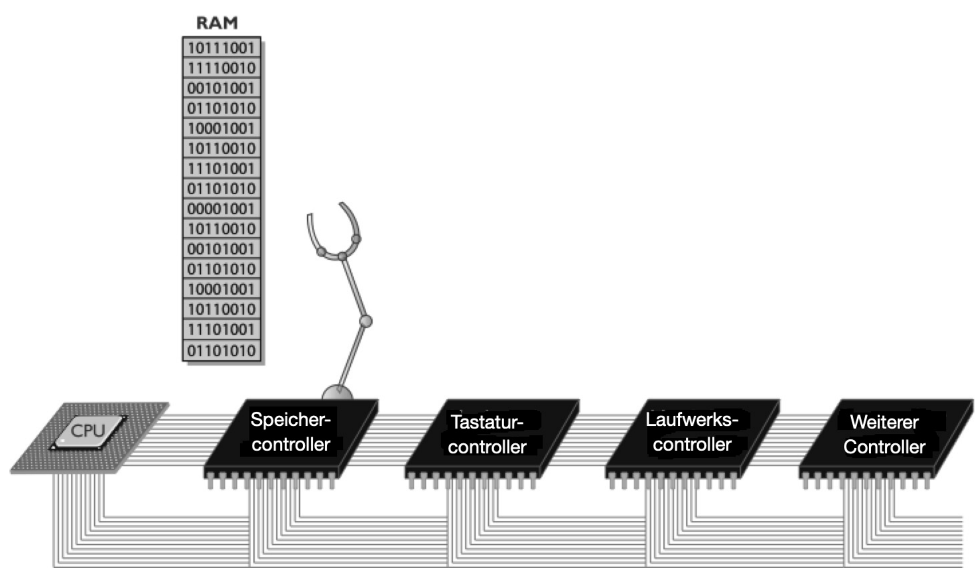


Abb. 5.2: Erweiterung von Daten- und Adressbus

Die ersten Mainboards waren mit Controller-Chips übersät. Abbildung 5.3 zeigt ein solches Mainboard, das mit Controller-Chips (und anderen Chips) vollgepackt ist.

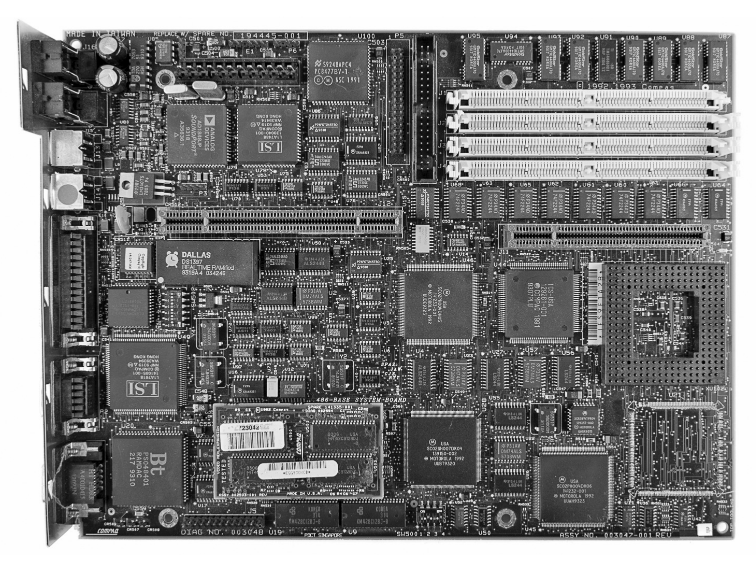


Abb. 5.3: Eines der ersten Mainboards, das mit Controller-Chips übersät ist

Im Laufe der Zeit entschlossen sich die Hersteller dazu, mehrere Controller in speziell entwickelten *Chipsätzen* zu kombinieren. Die ersten Chipsätze, wie der Intel 430VX in Abbildung 5.4, bestanden aus zwei Chips namens *Northbridge* und *Southbridge*. Viele Jahre lang, etwa von 1990 bis 2010, haben

die Chiphersteller paarweise aufeinander abgestimmte Northbridge- und Southbridge-Chipsätze angeboten. In heutigen CPUs sind Controller (wie Speicher- und Grafik-Controller) integriert. Fast alle Chipsätze bestehen nur noch aus einem Chip. Intel bezeichnet ihn als PCH (*Platform Controller Hub*). Abbildung 5.5 zeigt ein Mainboard, auf dem CPU und PCH erkennbar sind. AMD (und ein Großteil der PC-Branche) bezeichnen diesen Chip als Chipsatz.

Hinweis

Bis auf die energiesparendsten Modelle benötigen alle Chipsätze Kühlkörper oder Lüfter zur Kühlung. Die Lösungen sind häufig auf einem Chip integriert, dennoch ist es immer noch üblich, von einem »Chipsatz« zu sprechen (obwohl »Satz« eigentlich bedeutet, dass es mehrere sind).

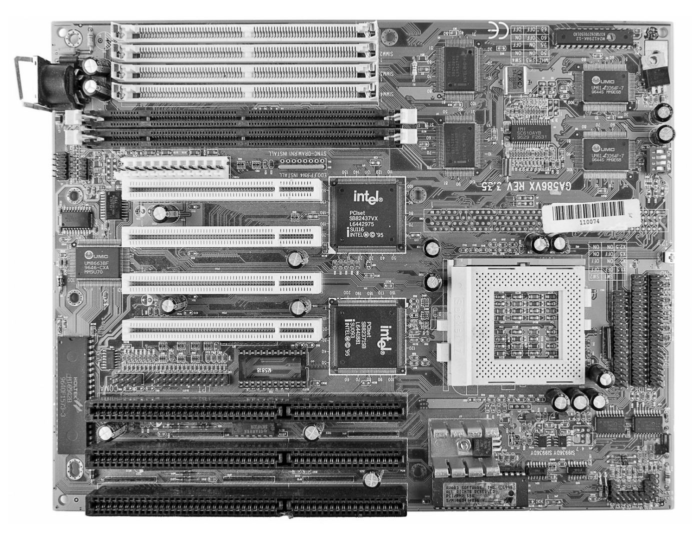


Abb. 5.4: Alter 430VX-Chipsatz mit Northbridge und Southbridge

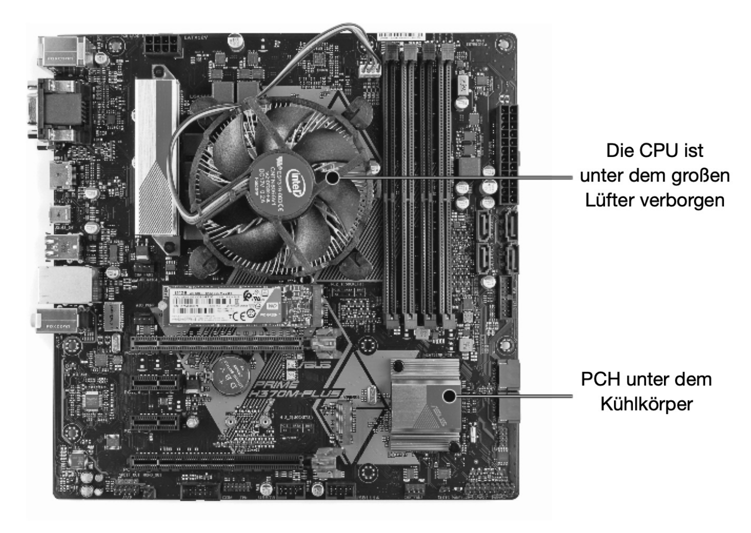


Abb. 5.5: Intel-CPU und PCH

Der Chipsatz erweitert den Datenbus zu den Komponenten im PC. Die CPU verwendet den Datenbus, um Daten von allen PC-Komponenten zu übernehmen und dorthin zu transportieren. Zwischen CPU, Chipsatz, RAM und anderen Komponenten im PC werden laufend Daten übertragen (Abbildung 5.6).

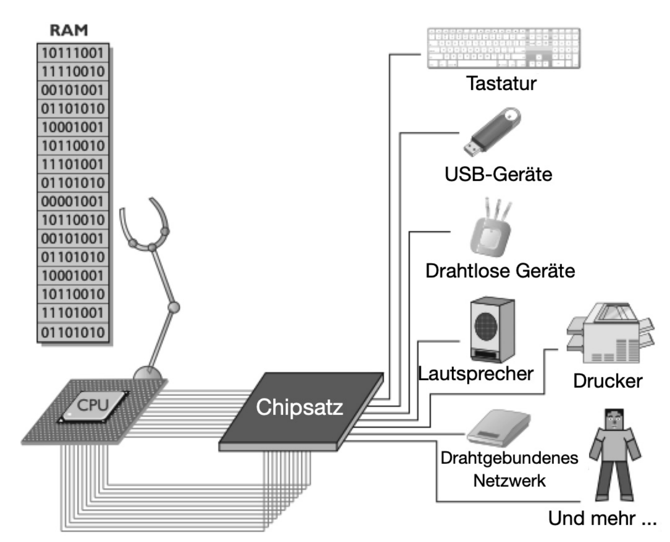


Abb. 5.6: Alles ist verbunden.

Das Konzept, dass der Adressbus von der CPU zur Kommunikation mit den Komponenten genutzt wird, ist nicht allzu schwierig zu verstehen, aber woher weiß sie, was sie diesen *mitteilen* muss? Woher kennt die CPU die ganzen verschiedenen Muster von Einsen und Nullen, die sie auf den Adressbus legen muss, um z.B. der Festplatte mitzuteilen, dass diese eine Datei übertragen soll? Um diese Vorgänge anschaulich zu begreifen, werden wir die Zusammenarbeit zwischen Tastatur und CPU eingehender betrachten.

5.1.1 Kommunikation mit der Tastatur

Die Tastatur stellt ein sehr gutes Beispiel für die Zusammenarbeit zwischen Bussen und Programmen zur Unterstützung der CPU bei ihren Aufgaben dar. Die Tastatur wird über einen speziellen Chip mit dem externen Datenbus verbunden, der *Tastatur-Controller* genannt wird. Sie sollten diesen Chip aber nicht auf dem Mainboard suchen, da er mittlerweile in den Chipsatz integriert wurde. An der Zusammenarbeit des Tastatur-Controllers mit der CPU hat sich aber in den letzten Jahrzehnten kaum etwas geändert. Daher eignet sich dieses Beispiel hervorragend zur Demonstration der Kommunikation zwischen der CPU und einer Komponente.

> **Hinweis**
>
> Oft sprechen Techniker über die verschiedenen Funktionen des Chipsatzes so, als würden diese Funktionen immer noch von unterschiedlichen Chips übernommen. Sie hören sie also z.B. von Speicher-, Tastatur-, Maus- und USB-Controllern sprechen, auch wenn es sich dabei durchweg einfach nur um Schaltkreise der CPU oder des Chipsatzes handelt.

Der Tastatur-Controller war einer der letzten Chips mit einer einzelnen Aufgabe, die mit in den Chipsatz integriert wurden. Abbildung 5.7 zeigt einen für die damalige Zeit typischen Tastatur-Controller. Dessen elektronische Funktion lässt sich vereinfacht wie in Abbildung 5.7 darstellen.

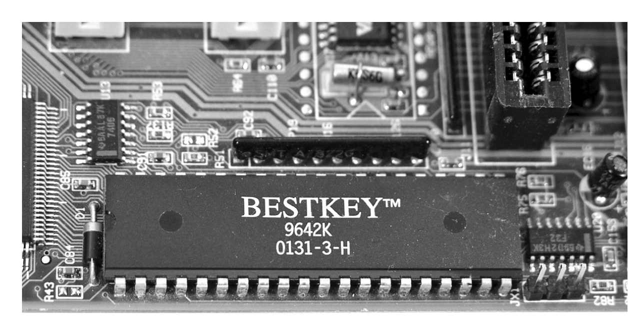


Abb. 5.7: Tastatur-Controller auf einem älteren Mainboard

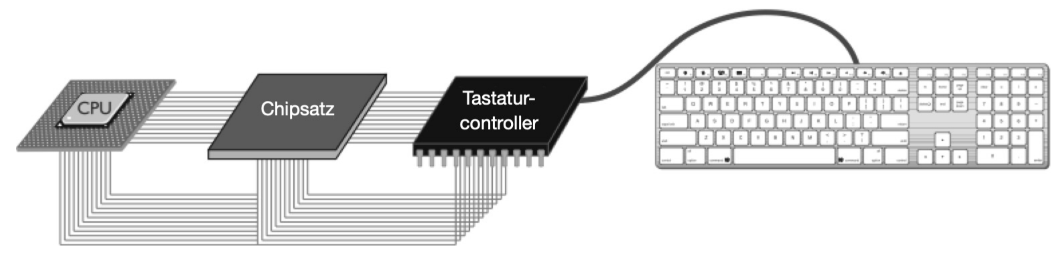


Abb. 5.8: Vereinfachte Darstellung der Funktion des Tastatur-Controllers

Immer dann, wenn Sie eine Taste drücken, registriert ein Chip in der Tastatur, um welche es sich handelt. Dieser Chip sendet dann eine Codefolge aus Nullen und Einsen an den Tastatur-Controller, den sogenannten *Scancode*. Allen Tasten der Tastatur sind jeweils eindeutige Scancodes zugeordnet. Der Tastatur-Controller speichert die Scancodes in eigenen Registern. Überrascht es Sie, dass selbst der einfache Tastatur-Controller und nicht nur die CPU Register besitzt? Das ist bei vielen Chips der Fall – nicht nur bei CPUs (Abbildung 5.9).

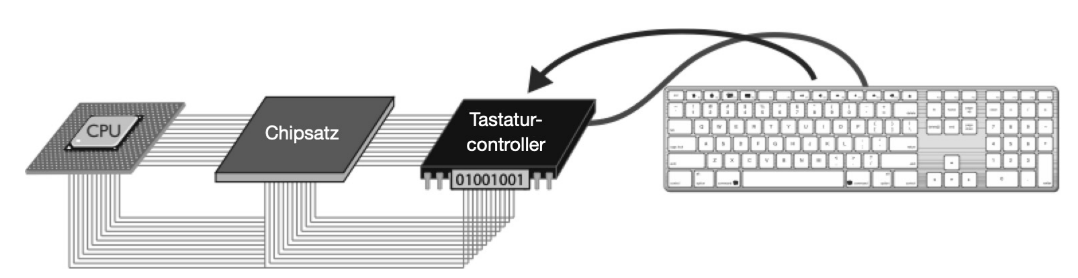


Abb. 5.9: Im Register des Tastatur-Controllers gespeicherte Scancodes

Wie kommt nun die CPU an die Scancodes im Tastatur-Controller? Da wir gerade dabei sind, wie kann die CPU der Tastatur den Befehl zur Änderung der Tastenwiederholrate (die Wiederholungsrate einer gedrückt gehaltenen Taste) oder zum An- oder Abschalten der Num-LED geben, um nur ein paar Beispiele für Aufgaben anzuführen, die eine Tastatur erledigen muss? Letztlich muss der Tastatur-Controller nicht nur auf einen, sondern auf mehrere Befehle reagieren können.

Der Tastatur-Controller nimmt Befehle auf die gleiche Weise wie der in Kapitel 4 vorgestellte Mikroprozessor entgegen. Können Sie sich noch daran erinnern, wie wir die Zahlen 2 und 3 mit dem 8088 addiert haben? Sie mussten bestimmte Befehle aus dem Codebuch des 8088 benutzen, um den Prozessor zur Addition aufzufordern und dafür zu sorgen, dass er die Lösung auf dem externen Datenbus abgelegt hat. Der Tastatur-Controller verfügt über ein eigenes Codebuch, das zwar viel einfacher als das der CPU, aber konzeptuell mit diesem vergleichbar ist. Um den innerhalb des Tastatur-Control-

lers gespeicherten Scancode zu ermitteln, muss die CPU den Befehl (oder die entsprechende Befehlsfolge) kennen, die den Tastatur-Controller dazu bringt, den Scancode des Zeichens auf dem externen Datenbus abzulegen, damit er von der CPU gelesen werden kann.

5.1.2 BIOS

Die CPU kann nicht wie von Zauberhand oder irgendwie automatisch mit jeder Komponente kommunizieren. Sie braucht irgendein unterstützendes Programm, das in den Speicher geladen wird und das sie über die Komponente informiert. Man spricht in diesem Zusammenhang vom *BIOS* (*Basic Input/Output System*). Die Programme, die für die Kommunikation der CPU mit Komponenten zuständig sind, werden Services oder auch *Gerätetreiber* genannt, wie Sie später in diesem Kapitel noch erfahren werden. Dies betrifft übrigens nicht nur die Tastatur. Tatsächlich benötigen *alle* Komponenten im Computer ein BIOS. Aber wir wollen uns hier einstweilen auf die Tastatur beschränken.

Wie das BIOS auf den Rechner gelangt

Wenn er das Codebuch der Tastatur kennt, dann kann ein begabter Programmierer das BIOS für eine Tastatur schreiben, denn Tastaturen sind relativ einfache Geräte. Damit stellt sich die Frage: Wo sollen die unterstützenden Programme gespeichert werden? Antwort: Sie könnten in das Betriebssystem integriert werden. Es ist praktisch, Programme im Betriebssystem unterzubringen, die mit der Rechnerhardware kommunizieren. Alle Betriebssysteme enthalten Code, der mit einer Tastatur, Maus und vielen anderen Hardwarekomponenten im Rechner kommunizieren kann.

Das ist schön und gut, wenn das Betriebssystem erst einmal läuft, aber wie steht es mit den brandneuen Komponenten, die Sie in einen neuen PC einbauen wollen? Wenn ein neues System aufgebaut wird, dann gibt es noch kein Betriebssystem! Die CPU muss auf das BIOS der wichtigsten Rechnerkomponenten zugreifen können, um mit ihnen kommunizieren zu können: nicht nur auf das der Tastatur, sondern auch auf das des Bildschirms, der Festplatten, der optischen Laufwerke, der USB-Anschlüsse und des RAMs. Der BIOS-Code kann also nicht auf einer Festplatte oder CD-ROM abgelegt werden, denn die wichtigen Komponenten müssen für den Zugriff der CPU jederzeit zur Verfügung stehen, noch bevor ein Massenspeichergerät oder ein Betriebssystem installiert wird.

Der ideale Speicherort für die unterstützenden Programme ist daher das Mainboard. Damit ist zwar dieses Problem gelöst, dafür entsteht aber ein anderes: Welches Speichermedium kann auf dem Mainboard verwendet werden? DRAM funktioniert nicht, weil die darin enthaltenen Daten jeweils beim Ausschalten des Rechners gelöscht werden. Es wird permanenter Programmspeicher benötigt, der unabhängig von anderen Peripheriegeräten funktioniert. Und dieser Speicher muss sich auf dem Mainboard befinden.

ROM

Mainboards speichern die den Tastatur-Controller unterstützenden Programme (neben anderen Programmen) in einem speziellen Bauteil, das *ROM* (*Read-Only Memory*) genannt wird. ROM-Chips speichern Programme bzw. Services genau wie RAM. ROM unterscheidet sich aber in zweierlei Hinsicht deutlich von RAM. Erstens ist der Speicher der ROM-Chips *nichtflüchtig*, sodass die hier gespeicherten Daten selbst dann nicht gelöscht werden, wenn der Computer abgeschaltet wird. Zweitens können ROM-Chips nur gelesen werden, sodass die dort gespeicherten Programme später nicht mehr geändert werden können.

Moderne Mainboards verwenden einen ROM-Typ, der auch *Flash-ROM* genannt wird und der auch die Daten in Ihrem Smartphone oder einem SSD-Laufwerk speichert. Das ist der Grund dafür, dass eine Aktualisierung des BIOS »ROM-Flashing« genannt wird (mehr dazu später). Abbildung 5.10 zeigt einen typischen Flash-ROM-Chip auf einem Mainboard.

Alle Mainboards besitzen einen Flash-ROM-Chip, den sogenannten *System-ROM-Chip*, der Code enthält, mit dessen Hilfe die CPU mit den Basiskomponenten des Rechners kommunizieren kann (Abbildung 5.11). Wie bereits erwähnt, enthält das System-ROM mehr als nur das BIOS des Tastatur-

Controllers. Es enthält auch Programme für die Kommunikation mit den Festplatten, optischen Laufwerken, Grafikkarten, USB-Anschlüssen und anderen Basiskomponenten auf dem Mainboard.

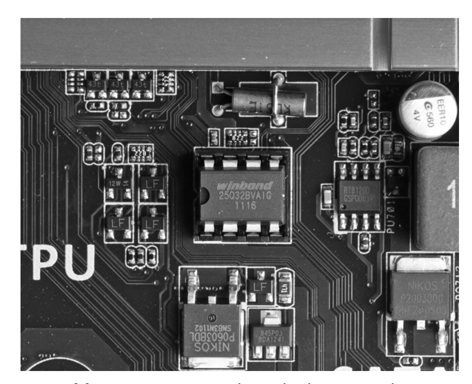


Abb. 5.10: Ein typischer Flash-ROM-Chip

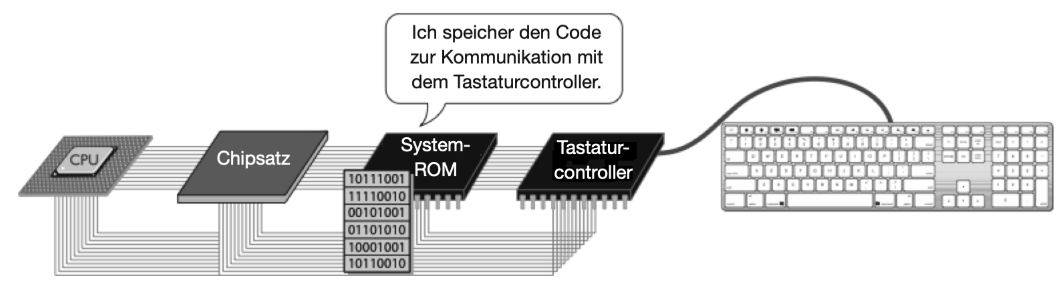


Abb. 5.11: Arbeitsweise des Flash-ROM-Chips

Um mit all diesen Hardwarekomponenten kommunizieren zu können, werden Hunderte kleiner Services (mit jeweils 2 bis 30 Codezeilen) benötigt. Diese im System-ROM-Chip des Mainboards untergebrachten Programme werden in ihrer Gesamtheit auch *System-BIOS* genannt (Abbildung 5.12). Techniker sprechen bei den in den unterschiedlichsten ROM-Chips gespeicherten Programmen von *Firmware*.

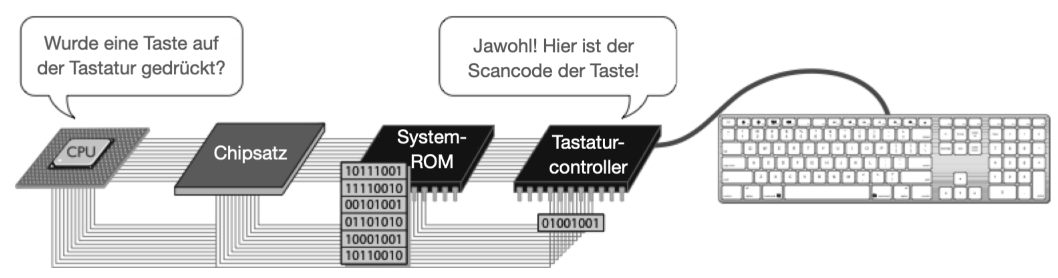


Abb. 5.12: CPU, die einen BIOS-Service ausführt

Wichtig

In ROM-Chips – egal ob Flash oder anderes ROM – gespeicherte Programme werden, im Gegensatz zu den auf löschbaren Datenträgern gespeicherten Programmen, die als *Software* bezeichnet werden, auch *Firmware* genannt.

System-BIOS-Unterstützung

Jedes System-BIOS muss zwei Arten von Hardware unterstützen. Erstens unterstützt das System-BIOS Hardwarekomponenten, die sich nie ändern, wie z.B. die Tastatur. (Sie können zwar die Tastatur austauschen, aber nicht den in den Chipsatz eingebauten Tastatur-Controller.) Ein weiteres Beispiel für Hardwarekomponenten, an denen sich nie etwas ändert, ist der PC-Lautsprecher (der winzige Lautsprecher, der manchmal Pieptöne ausgibt, nicht die Lautsprecher, über die Musik ausgegeben wird). Der System-ROM-Chip speichert das BIOS für diese und andere Komponenten, die sich nie ändern.

Zweitens unterstützt das System-BIOS all jene Hardwarekomponenten, die sich immer wieder einmal ändern können. Dies sind unter anderem RAM (der Speicher kann erweitert werden), Festplatten (Sie können sie durch größere Laufwerke ersetzen oder ein SSD-Laufwerk einbauen). Im System-ROM-Chip ist zwar das BIOS für diese Geräte gespeichert, aber das System braucht noch einen anderen Ort, an dem es Detailinformationen über bestimmte Hardwarekomponenten ablegen kann. Auf diese Weise kann ein System zwischen Laufwerken wie einer Festplatte des Modells Western Digital Blue mit 4 TB und einer SSD des Modells Samsung 860 EVO-SSD mit 2 TB unterscheiden und doch beide Laufwerke direkt unterstützen.

UEFI

Moderne Systeme setzen ein BIOS ein, das den Namen *UEFI* (*Unified Extensible Firmware Interface*) trägt. Hier sind einige der Vorteile, die UEFI gegenüber dem ursprünglichen BIOS aufweist:

- UEFI unterstützt das Booten von Dateisystemen, die größer als 2,2 TB sein dürfen.
- UEFI kann im 32-Bit- oder 64-Bit-Modus starten, was es den Herstellern ermöglicht, bei der Einrichtung und Diagnose viele Features anzubieten.
- UEFI erledigt sämtliche beim Start erforderlichen Aufgaben.
- UEFI ist nicht auf 16-BIT-x86-Firmware angewiesen.

Alle aktuellen Systeme verwenden UEFI und bieten gleichzeitig Unterstützung für alte BIOS-Services, falls Sie an alten Spielen interessiert sind. Noch aber nutzen Myriaden älterer Systeme das betagte BIOS. Viele Techniker bezeichnen die unterstützende Software nach wie vor als BIOS, obwohl UEFI und BIOS natürlich nicht dasselbe sind. Es gibt übrigens keine Standardisierung der Aussprache des Begriffs »UEFI«. Microsoft buchstabiert es: »U-E-F-I«. Andere sagen hingegen »Ju-Fi« oder mit englischer Betonung »Ju-Fei«.

5.2 CMOS und RTC

Weil das BIOS im ROM gespeichert ist und ROM nur lesbar ist, benötigt es einen Ort, um die Einstellungen zu speichern, damit sie nicht bei jedem Start des Computers erneut eingegeben werden müssen. Dieser Ort ist ein wenig RAM, das von einer kleinen Batterie mit Spannung versorgt wird, damit es auch bei ausgeschaltetem PC funktioniert. Wir bezeichnen diesen Speicher als *CMOS-Chip* (*Complementary Metal-Oxide Semiconductor*). Das CMOS speichert nicht nur die verschiedenen BIOS-Einstellungen, sondern fungiert außerdem als Echtzeituhr (*Real-Time Clock*, RTC) des Systems, damit Sie nicht bei jedem Start die Uhrzeit einstellen müssen.

Vor vielen Jahren handelte es sich beim CMOS um einen eigenständigen Chip auf dem Mainboard (siehe Abbildung 5.13). Heute ist das CMOS fast immer Teil des Chipsatzes. Die im CMOS gespeicherten Informationen sind für die Funktionsfähigkeit des Rechners unbedingt erforderlich!

Wenn die über eine bestimmte Hardwarekomponente (oder über deren ausgefeilteren Eigenschaften) im CMOS gespeicherten Daten nicht mit den Spezifikationen der tatsächlich vorhandenen Hardware übereinstimmen, dann kann der Rechner nicht auf diese Hardwarekomponente (oder deren anspruchsvollere Funktionen) zugreifen. Es ist unabdingbar, dass die entsprechenden Informationen zutreffend sind. Wenn eine der bereits genannten Hardwarekomponenten geändert wird, dann muss das CMOS aktualisiert werden, damit es diese Änderungen widerspiegelt. Sie müssen daher wissen, wie Sie die im CMOS-Chip gespeicherten Daten ändern können.

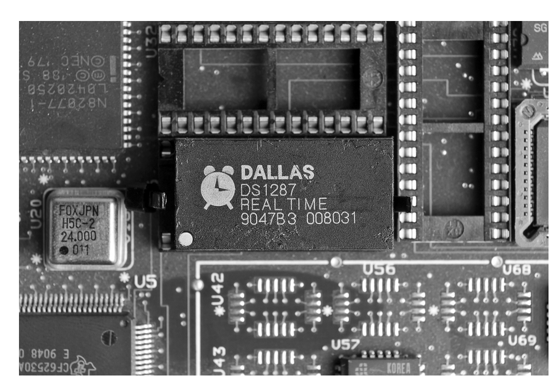


Abb. 5.13: Ein CMOS-Chip alter Schule

Wichtig

Alle Details zum UEFI und CMOS, die Sie für die Prüfung stundenlang auswendig lernen müssen, betreffen nur PCs und Linux-Rechner. Apples Computer verwenden ebenfalls ein EFI und ein CMOS, die Rechner sind jedoch von Grund auf als einheitliche Systeme konzipiert und Apple hat bereits alle erforderlichen Aufgaben erledigt. Sie können einen Rechner mit macOS einfach so benutzen.

Alle PCs verfügen über ein Programm im System-ROM, das *CMOS-Setup* oder *System-Setup* genannt wird. Mit diesem Programm können Daten im CMOS-Chip gelesen und geändert werden. Wenn Sie ein völlig neues System starten, auf dem noch kein Betriebssystem installiert ist, wird zunächst immer etwas wie in Abbildung 5.14 angezeigt.

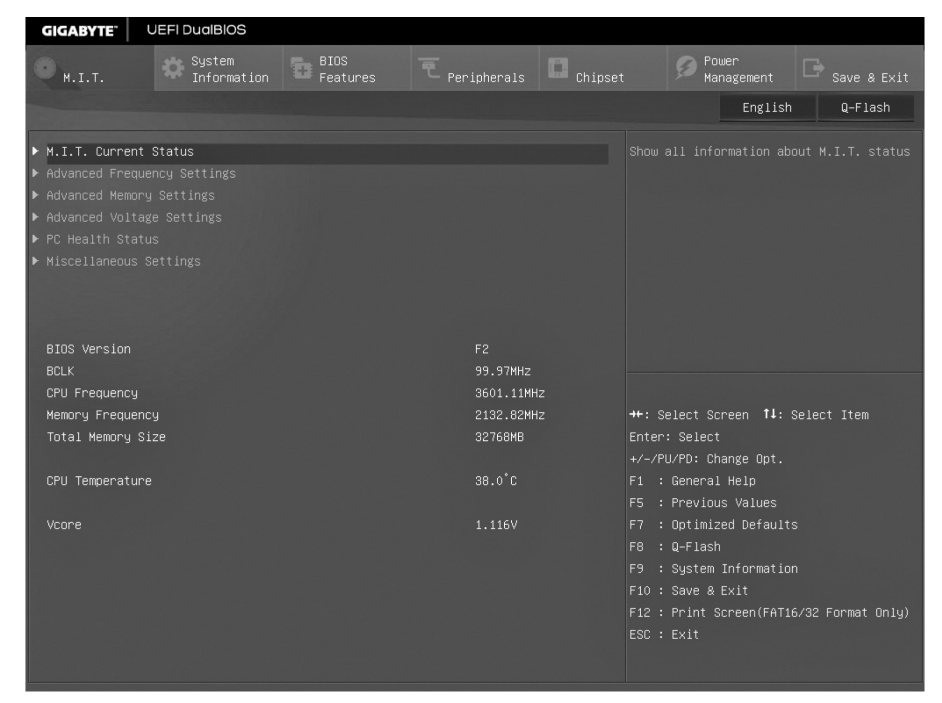


Abb. 5.14: System-Setup-Programm von Gigabyte

Nachdem ein Betriebssystem installiert worden ist, erscheint diese Anzeige nicht mehr. Gleich erfahren Sie, wie Sie darauf zugreifen können

Hinweis

Die Begriffe *CMOS-Setup*, *CMOS* und *System-Setup* werden heute austauschbar genutzt. Man hört manchmal auch den Begriff *BIOS-Setup-Dienstprogramm*. Die meisten Techniker sprechen einfach vom CMOS.

UEFI-Setup-Programm mit grafischer Benutzeroberfläche

Abbildung 5.15 zeigt ein typisches, einfaches Setup-Programm mit grafischer Oberfläche. Es verfügt über einen einfachen und einen erweiterten Modus. Viel kann man hier im einfachen Modus nicht einstellen: Sie können lediglich Informationen über die installierten Komponenten anzeigen, eine von drei vorgegebenen Optionen zur Geschwindigkeitsoptimierung auswählen und die Bootreihenfolge ändern.

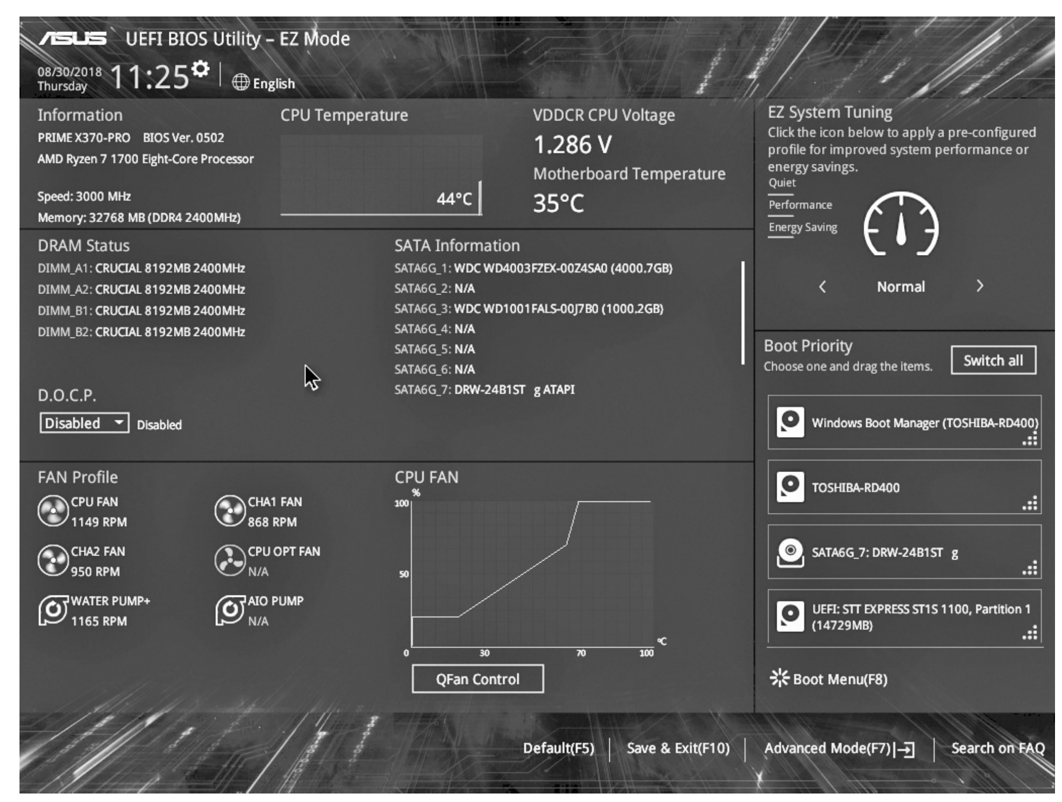


Abb. 5.15: UEFI-System-Setup-Programm von ASUS

Wenn Sie die Option für den erweiterten Modus auswählen, stehen Ihnen erheblich vielseitigere Werkzeuge zum Ändern der Konfiguration zur Verfügung (Abbildung 5.16). Auf der Hauptregisterkarte werden Informationen über verschiedene BIOS-Komponenten angezeigt, wie Details zum eingebauten RAM und zur CPU-Geschwindigkeit sowie einige Optionen zum Ändern von Sprache, Datum und Uhrzeit. (Manche Setup-Programme zeigen hier Informationen über die installierten Laufwerke an; dieses UEFI zeigt solche Informationen an anderer Stelle an.)

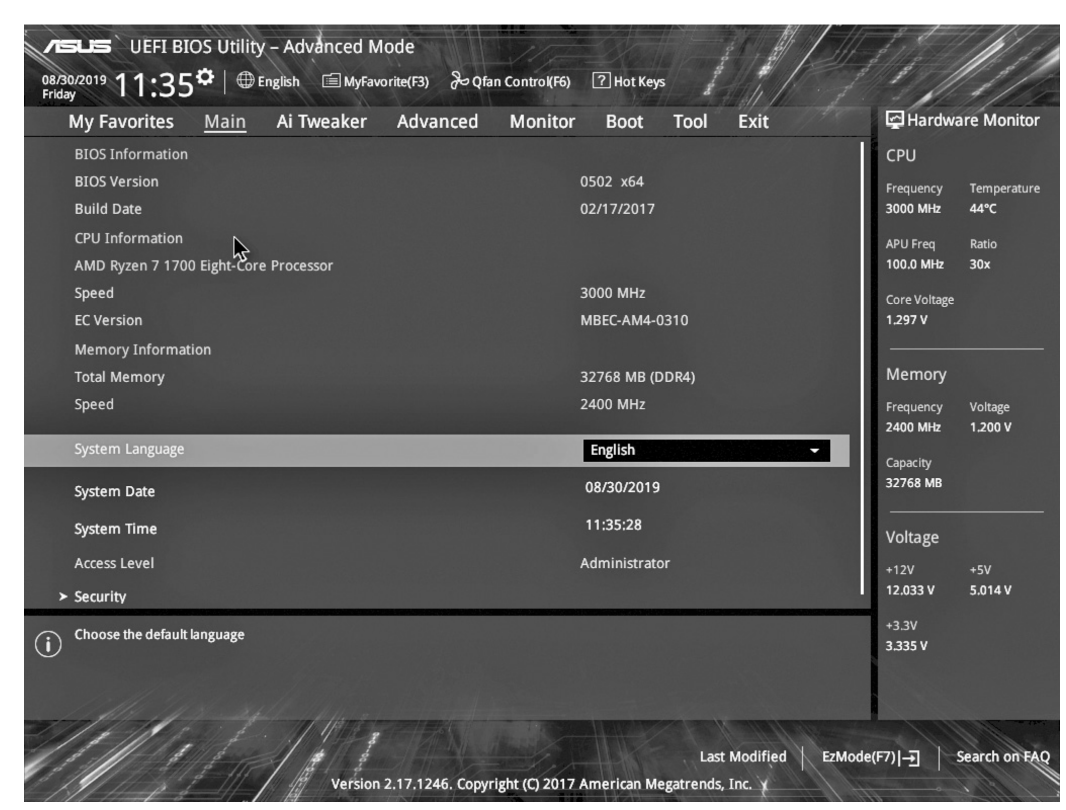


Abb. 5.16: Erweiterter Modus

Auf der Hauptregisterkarte können auch einfache Sicherheitseinstellungen vorgenommen werden, indem Sie ein Administrator- oder Benutzerkennwort vergeben. (Die Standardeinstellung für die Zugriffsrechte des abgebildeten UEFI-BIOS ist Administrator. Klicken Sie auf die zugehörige Schaltfläche, um die Zugriffsrechte zu ändern. Die Bedienoberflächen grafischer UEFI-Setup-Programme unterscheiden sich ein wenig voneinander, ähnliche Optionen sind jedoch in allen zu finden.)

Durch ein Administratorkennwort ist der Zugriff auf das Setup-Programm geschützt. Zum Starten eines Betriebssystems muss ein Benutzerkennwort eingeben werden. Vergeben Sie ein BIOS/UEFI-Kennwort, wenn ein PC leicht für jedermann zugänglich ist, wie etwa auf einer Messe oder in einer öffentlichen Bibliothek. Ein BIOS/UEFI-Kennwort schützt davor, dass irgendjemand unerwünschte Änderungen an einem zugänglichen System vornimmt.

Auf den übrigen Registerkarten wird es erst richtig interessant. So kann man sich etwa in der Schwarzen Kunst der Übertaktung von CPU und RAM üben (Abbildung 5.17) und Taktvervielfachung, Taktfrequenz, Spannungen und anderes ändern, wenn man die Registerkarte AI TWEAKER auswählt. Hier sind Sie genau richtig, um eine neue CPU durchzuschmoren!

Auf der Registerkarte mit erweiterten Einstellungen (Abbildung 5.18) finden sich Informationen über CPUs, Festplatten, optische Laufwerke und die weiteren eingebauten Komponenten, wie etwa USB-Anschlüsse. In den verschiedenen Unterkategorien dieser Registerkarte können Sie Laufwerkseinstellungen konfigurieren, Geräte aktivieren/deaktivieren und vieles mehr.

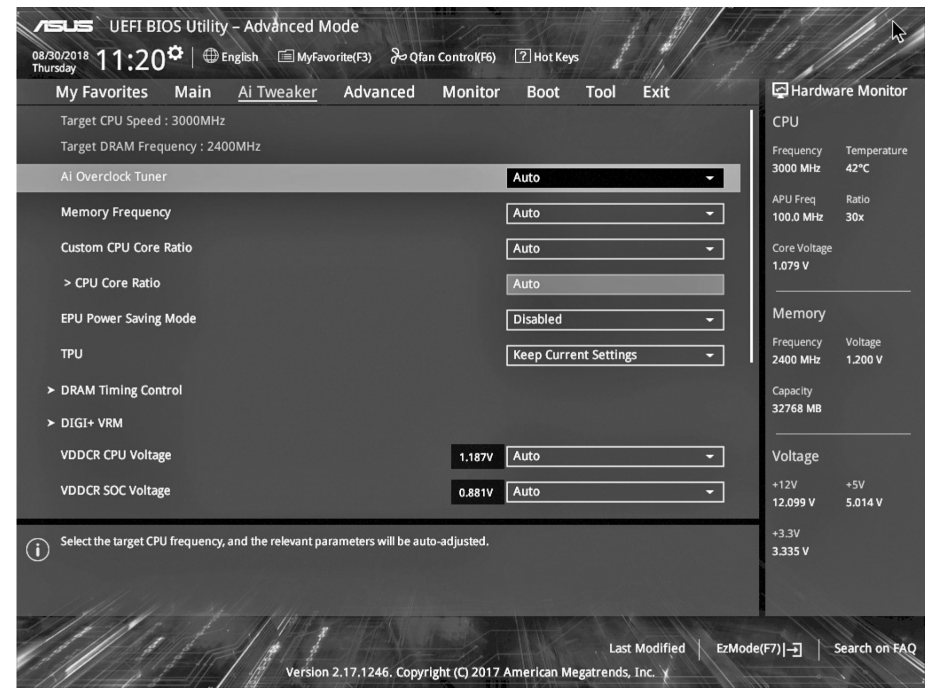


Abb. 5.17: Übertaktung und Taktvervielfachung

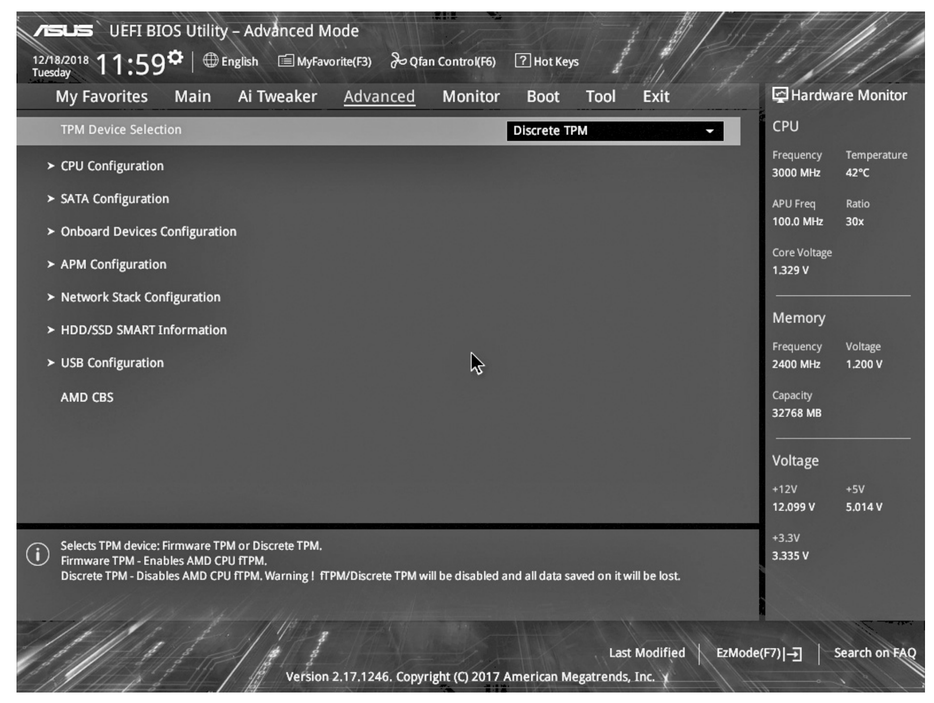


Abb. 5.18: Erweiterte Einstellungen

Auf einer weiteren Registerkarte namens Monitor (Abbildung 5.19) werden die Temperaturen von CPU und Mainboard, Lüftergeschwindigkeiten und Spannungen angezeigt. Das Verhalten der Gehäuselüfter ist hier ebenfalls konfigurierbar. Auf all diese Informationen greifen die eingebauten Diagnosewerkzeuge für das Mainboard und das Gesamtsystem zurück.

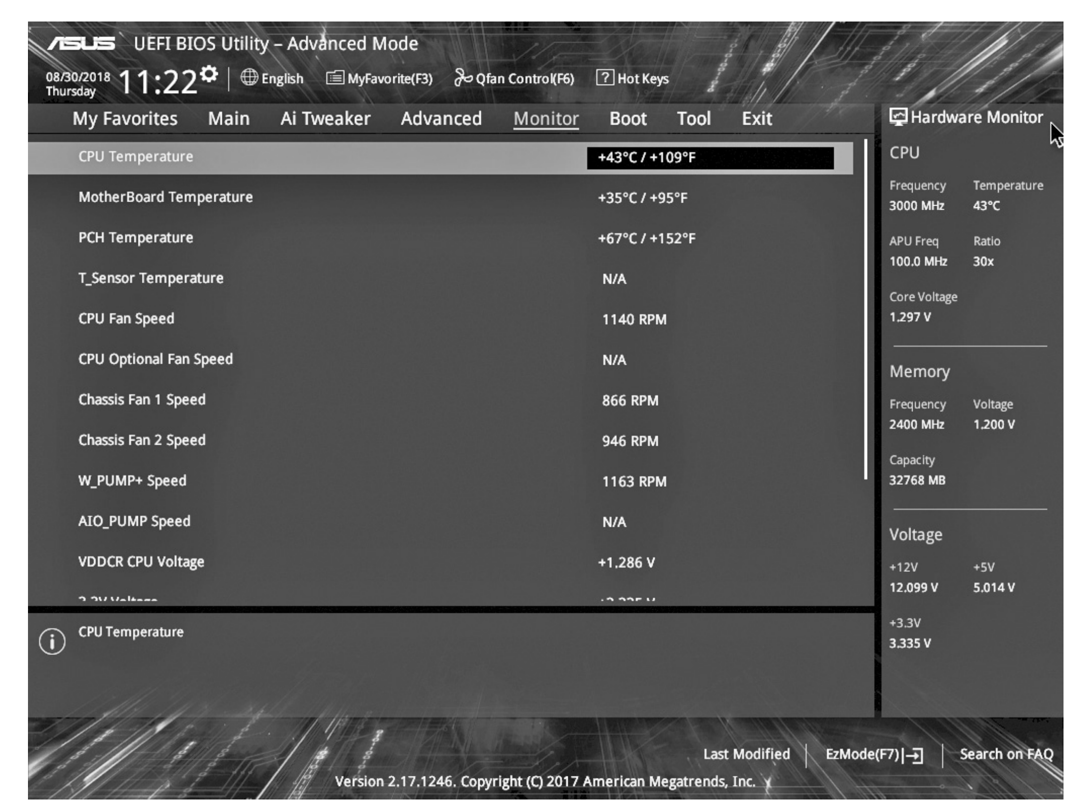


Abb. 5.19: Überwachung von Temperaturen und Lüftergeschwindigkeiten

Die Registerkarte Boot (Abbildung 5.20) gestattet das Ändern der Booteinstellungen. Hier können Sie die für das Mainboard gültige Bootreihenfolge festlegen. (Mehr dazu im Abschnitt 5.4.4, *Der Bootprozess*, später in diesem Kapitel.) Sie können unter anderem festlegen, wie das System reagieren soll, wenn das Booten fehlschlägt.

Auf der Registerkarte Tool (Abbildung 5.21) sind einige sehr wichtige Funktionalitäten zu finden. Das Werkzeug EZ Flash 3 ermöglicht eine Aktualisierung der Firmware des Mainboards. Details dazu finden Sie im Abschnitt 5.6, *Flash-ROM aktualisieren*, später in diesem Kapitel. Diese Registerkarte zeigt außerdem Informationen über das RAM an. Hierbei handelt es sich um die SPD-Option (*Serial Presence Detect*), die Sie bereits aus Kapitel 4, *RAM*, kennen.

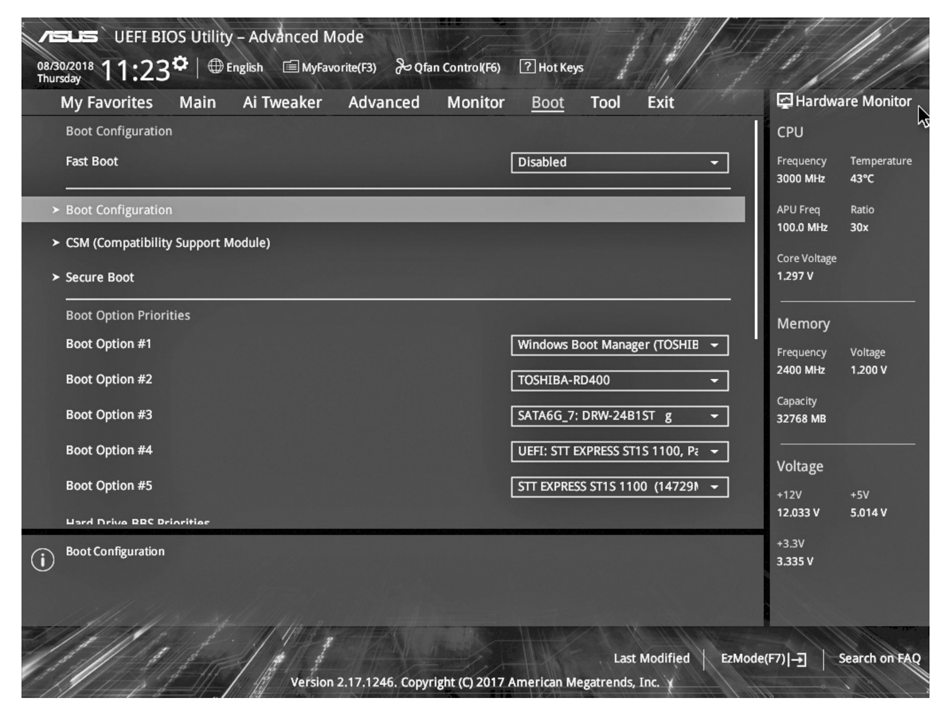


Abb. 5.20: Registerkarte BOOT

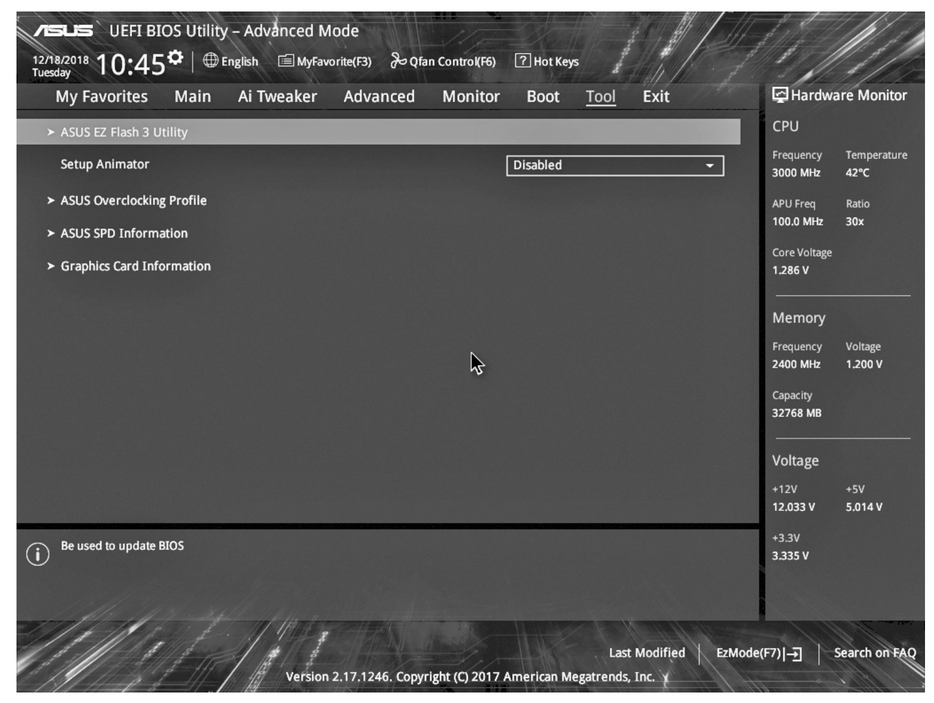


Abb. 5.21: Registerkarte TOOL

Textbasiertes UEFI-Setup-Programm

Bei diesem zweiten Durchgang kommt ein UEFI-Mainboard eines tragbaren Computers mit Intel-Prozessor zum Einsatz. Achten Sie bei den Abbildungen auf die dargestellten Optionen. Auf Funktionen, die im Setup-Programm mit grafischer Oberfläche nicht vorhanden sind, weise ich hin.

Die Registerkarte INFORMATION (Abbildung 5.22) zeigt unmittelbar Daten über CPU und RAM sowie kryptische Infos über die Festplatte an. Auf anderen Registerkarten finden sich weitere Informationen.

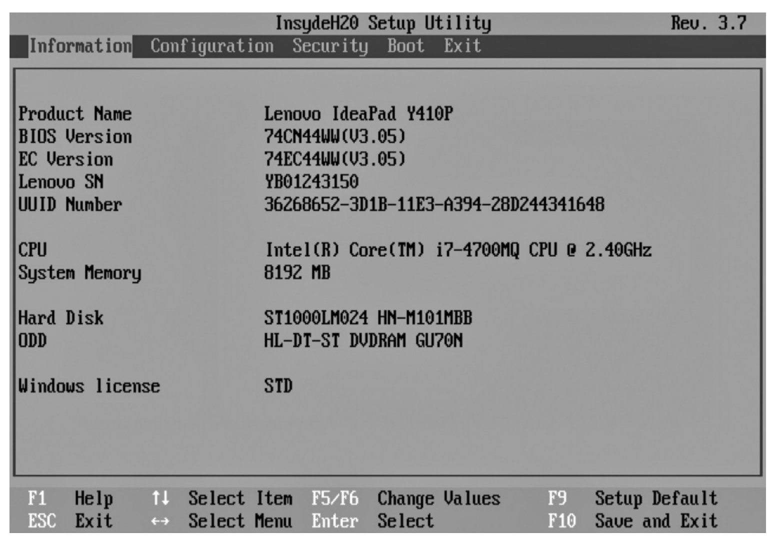


Abb. 5.22: Registerkarte INFORMATION

Die Registerkarte CONFIGURATION (Abbildung 5.23) zeigt eine Reihe eingebauter Geräte an, die Sie hier konfigurieren und aktivieren bzw. deaktivieren können. Da es sich hier um einen Laptop handelt, gibt es die Möglichkeit, das drahtlose Netzwerk ein- bzw. auszuschalten.

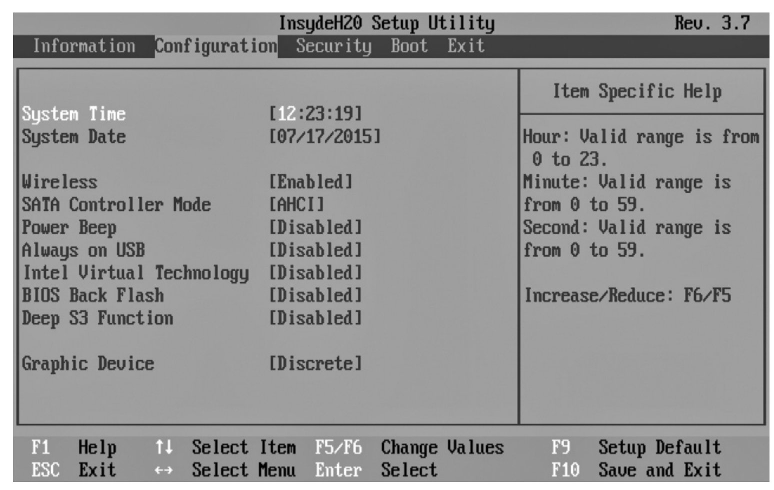


Abb. 5.23: Registerkarte CONFIGURATION

Hier gibt es zwei interessante Optionen, die in anderen Kapiteln ausführlich behandelt werden, an dieser Stelle aber kurz erwähnt werden sollen. Die Option INTEL VIRTUAL TECHNOLOGY aktiviert bzw. deaktiviert die Unterstützung virtueller Maschinen.

Eine *virtuelle Maschine* ist ein leistungsfähiges Programm, das es Ihnen gestattet, eine zweite (oder dritte oder vierte), softwarebasierte Maschine auf Ihrem physischen PC zu betreiben. Es bildet Mainboard, Festplatten, RAM, Netzwerkkarten u.v.m. in Software nach und ist genauso leistungsstark wie ein echter PC. Um eine solche virtuelle Maschine auszuführen, ist allerdings ein äußerst leistungsfähiger PC erforderlich – letzten Endes versuchen Sie ja schließlich, mehrere PCs gleichzeitig zu betreiben.

Um dies zu ermöglichen, haben die CPU-Hersteller eine *von der Hardware unterstützte Virtualisierung* entwickelt. Die Intel-Version heißt *Intel Virtualization Technology* (oder kurz *Intel VT*) und AMD hat die eigene Version *AMD Virtualization* (*AMD-V*) genannt. Diese Technologie unterstützt die virtuelle Maschine dabei, die Hardware effizienter zu nutzen und wird vom BIOS gesteuert. Diese Funktionalität ist im BIOS standardmäßig deaktiviert, Sie sollten sie daher hier aktivieren, wenn Sie eine virtuelle Maschine mit Hardware-Unterstützung betreiben möchten.

Hinweis

In Kapitel 22, *Virtualisierung*, kommen virtuelle Maschinen ausführlich zur Sprache. Bleiben Sie dran!

Dieser spezielle Laptop besitzt dank des Core-i7-Prozessors eine integrierte Grafik, verfügt außerdem aber auch über eine für Videospiele geeignete eigenständige Grafikkarte. Die auf »Discrete« (separat) eingestellte Option für die Grafikkarte bedeutet, dass möglichst die eigenständige Grafikkarte verwendet werden soll. Dadurch steigt zwar im Vergleich zur in die CPU integrierten Grafikkarte der Energieverbrauch an, aber das Spielen macht viel mehr Spaß!

Hinweis

In Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*, werden Grafikkarten moderner Systeme (und deren Eignung für Spiele) ausführlich vorgestellt.

Die Registerkarte SECURITY (Abbildung 5.24) bietet gegenüber der Hauptregisterkarte von AMD-Systemen viele weitere Optionen zur Konfiguration der BIOS-Sicherheitseinstellungen. Neben Administrator- und Benutzerkennwort können weitere Kennwörter für verschiedene Laufwerke vergeben werden.

Bei der auf der Registerkarte erkennbaren Funktion SECURE BOOT handelt es sich um ein UEFI-Protokoll, das für einen sicheren Bootprozess sorgen soll, indem es korrekt signierte Software erfordert. Das betrifft sowohl die eigentliche Bootsoftware als auch Software zur Unterstützung bestimmter wichtiger Komponenten. (Weitere Informationen dazu finden Sie im Abschnitt 5.3.2, *Gerätetreiber*, der gleich folgt.) Secure Boot erfordert eine Intel-CPU, ein UEFI-BIOS und ein dafür ausgelegtes Betriebssystem, wie etwa Windows.

Hinweis

Secure Boot ist ein Beispiel für eine Software, die eine *Laufwerkverschlüsselung* nutzt. Heutzutage werden eine Reihe unterschiedlicher Verschlüsselungsmethoden eingesetzt, um die verschiedensten Vorgänge und Daten zu schützen. Dabei werden im Wesentlichen die Daten so durcheinandergewürfelt, dass die bösen Buben nichts mehr damit anfangen können. Ich komme später im Buch darauf zurück. In Kapitel 9, *Vorbereitung und Wartung von Festplatten*, gehe ich ausführlich auf die Laufwerkverschlüsselung ein.

Auf der Registerkarte BOOT (Abbildung 5.25) können Sie Booteinstellungen vornehmen. Hier können Sie auch die Unterstützung für das Booten von USB-Laufwerken konfigurieren. Allerdings unter-

scheidet sich die Ansicht etwas von der vorhin verwendeten grafischen Oberfläche. Weitere Erläuterungen finden Sie im nachfolgenden Abschnitt 5.4.4, *Der Bootprozess*.

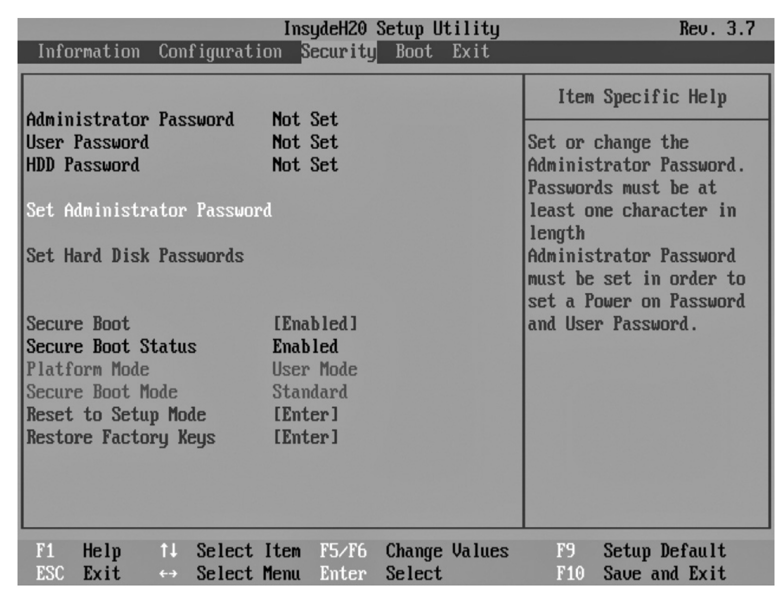


Abb. 5.24: Registerkarte SECURITY

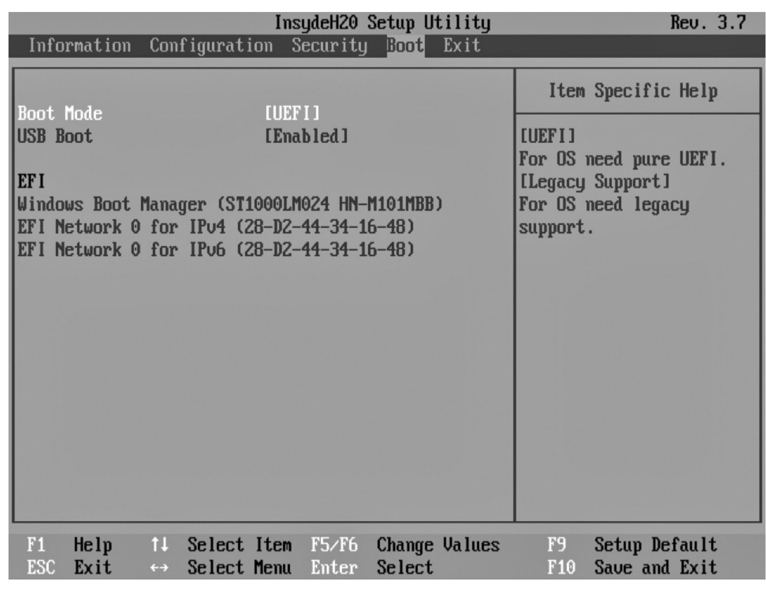


Abb. 5.25: Registerkarte BOOT

Weitere BIOS-Sicherheitseinstellungen

Mainboard- und BIOS/UEFI-Hersteller sowie Programmierer haben im Laufe der Jahre alle möglichen Sicherheitsfunktionen entwickelt. In diesem Abschnitt werden einige davon vorgestellt, denen

Sie womöglich bei dem einen oder anderen Mainboard in der Praxis (oder in einer gewissen, in naher Zukunft bevorstehenden Prüfung) begegnen werden.

Einbruchserkennung beim Gehäuse Viele Mainboards unterstützen mit der *Chassis Intrusion Detection* eine Art Einbruchsicherung für das Rechnergehäuse (*Chassis*). Kompatible Gehäuse verfügen über einen Schalter, der immer dann ausgelöst wird, wenn das Gehäuse geöffnet wird. Wenn diese Funktion auch vom Mainboard unterstützt wird und für die richtige Verbindung zwischen dem Mainboard und dem Schalter am Gehäuse gesorgt wird, dann zeichnet das CMOS auf, ob das Gehäuse geöffnet wurde, und zeigt beim anschließenden Rechnerstart eine entsprechende Meldung auf dem Bildschirm an. Wie abgefahren ist das denn?

LoJack Bei einigen PC-Herstellern gibt es im BIOS eine Sicherheitsfunktion namens LoJack, die es Ihnen erlaubt, einen gestohlenen PC zu orten, darauf einen Keylogger zu installieren oder ihn sogar aus der Ferne abzuschalten.

TPM (Trusted Platform Module) TPM (*Trusted Platform Module*) fungiert als sicherer Kryptoprozessor und damit handelt es sich sozusagen um eine Hardwareplattform zur Beschleunigung kryptographischer Funktionen und die sichere Speicherung der zugehörigen Informationen. Die TPM-Spezifikation wird von der *Trusted Computing Group* veröffentlicht, bei der es sich um eine Organisation handelt, zu dessen Mitgliedern namhafte Firmen wie Intel, Microsoft, AMD, IBM, Lenovo, Dell, Hewlett-Packard und viele andere zählen.

Bei dem TPM-Modul kann es sich um eine kleine Platine, die in das Mainboard eingesetzt wird, oder um Funktionen handeln, die direkt in den Chipsatz integriert wurden. Das CMOS-Setup-Programm enthält üblicherweise Einstellungen, über die sich TPM aktivieren oder deaktivieren lässt.

Auch wenn sich die TPM-Funktionen für vielfältige kryptographische Aufgabenstellungen nutzen lassen, werden sie vorwiegend zur Verschlüsselung von Festplattendaten genutzt. Die in Windows enthaltene BitLocker-Laufwerkverschlüsselung lässt sich mit einem TPM z.B. beschleunigen und sicherer gestalten, weil das zur Verschlüsselung verwendete Kennwort in der unzugänglichen TPM-Hardware und nicht auf einem externen Speicherstick abgelegt wird. Zu den weiteren möglichen Einsatzgebieten von TPMs zählen mit *DRM* (*Digital Rights Management*) die digitale Rechteverwaltung, die Zugriffssteuerung für Netzwerke, die Überwachung der Ausführung von Anwendungen und der Kennwortschutz.

Wichtig

Fragen zu BIOS-Sicherheitseinstellungen können TPM, Kennwörter, Secure Boot, Einbruchserkennung und Laufwerkverschlüsselung betreffen.

Beenden und Einstellungen speichern

Natürlich können Sie bei allen System-Setup-Programmen Einstellungen speichern oder das Programm ohne Speichern verlassen (Abbildung 5.26). Die letztere Option ist nützlich, falls Sie ein wenig im BIOS herumspielen möchten, ohne dabei Schaden anzurichten. Probieren Sie das ruhig aus!

Das CMOS-Setup-Programm würde alle Erfordernisse eines modernen Systems im Hinblick auf das BIOS erfüllen, wenn die Hersteller einfach damit aufhören würden, neue Komponenten zu entwickeln. Das wird natürlich nicht passieren, deshalb wollen wir jetzt jene Komponenten betrachten, die selbst ein BIOS haben müssen, das anderweitig geladen werden muss.

Hinweis

Wenn jemand die UEFI-Einstellungen ändern möchte, um maximale Leistung (Übertaktung) oder minimalen Energieverbrauch (Untertaktung) zu erzielen, steht dafür in manchen Setup-Programmen ein Feature zur Verfügung, mit dem sich verschiedene benutzerdefinierte Einstellungen speichern lassen. Sie werden meist als Voreinstellungen oder als Profil bezeichnet – im Wesentlichen handelt es sich um eine »Sichern als«-Option. Wenn nach einer Änderung irgendetwas nicht mehr richtig funktioniert, kann man

das Setup-Progamm erneut starten, weitere Änderungen vornehmen und es noch einmal versuchen. Wenn man mit dem Experimentieren fertig ist, wählt man das Profil eines stabilen Rechners, um vernünftig arbeiten zu können. Im Abschnitt 5.5, *Wartung von BIOS/UEFI und CMOS*, erfahren Sie mehr zum Thema Wiederherstellung.

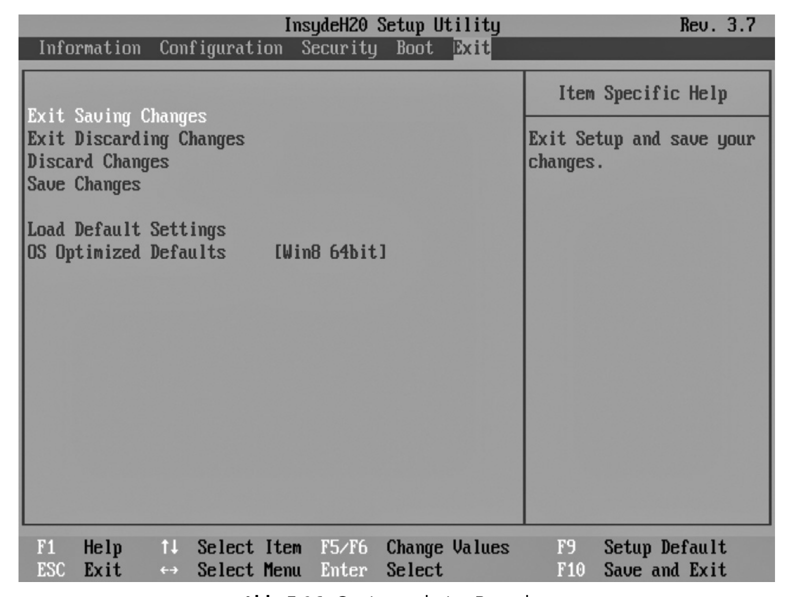


Abb. 5.26: Optionen beim Beenden

5.3 Optionales ROM und Gerätetreiber

Jede Hardwarekomponente in Ihrem Computer benötigt irgendein Programm, das der CPU mitteilt, wie sie mit ihr kommunizieren kann. Als IBM vor Jahrzehnten den PC entwickelt hat, konnte es natürlich unmöglich alle für sämtliche nur erdenklichen Hardwarekomponenten erforderlichen BIOS-Routinen in den System-ROM-Chip einprogrammieren. Wie soll das auch gehen? Die meisten der heute verwendeten Komponenten gab es damals noch gar nicht! Als die Programmierer das erste BIOS schrieben, gab es z.B. keine Netzwerkkarten, Mäuse oder Soundkarten. Den damaligen PC-Entwicklern bei IBM war klar, dass sie nicht wissen konnten, welche neuen Hardwarekomponenten irgendwann einmal entwickelt werden würden, und sahen daher einige Möglichkeiten vor, die BIOS-Routinen um eigene Programme zu erweitern. Es gibt zwei Möglichkeiten, eigene BIOS-Routinen mitzubringen: optionales ROM und Gerätetreiber. In den folgenden Abschnitten werden wir diese beiden Alternativen eingehender betrachten.

5.3.1 Optionales ROM

Die erste Methode, eigenes BIOS zur Verfügung zu stellen, besteht darin, das BIOS in die Hardwarekomponente selbst zu integrieren. Sehen Sie sich die Steckkarte in Abbildung 5.27 an. Es handelt sich dabei um einen Serial-ATA-RAID-Festplatten-Controller – also eine Karte, mit deren Hilfe Sie weitere Festplatten in einen PC integrieren können. Der Chip in der Mitte mit den seitlichen Anschlusskontakten ist ein Flash-ROM mit dem BIOS der Karte. Das System-BIOS weiß nicht, wie es mit dieser Karte kommunizieren kann, aber das macht nichts, weil die Karte ihr eigenes BIOS mitbringt, einen sogenannten optionalen ROM-Chip (Option ROM).

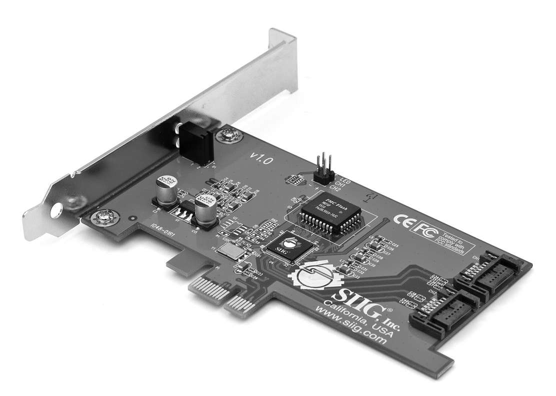


Abb. 5.27: Optionales ROM auf einer Erweiterungskarte

Ein Zusatz-BIOS in einem optionalen ROM meldet sich beim Booten meist mit bestimmten Informationen und signalisiert dadurch sein Vorhandensein. Abbildung 5.28 zeigt ein typisches Beispiel für die Meldung eines optionalen ROMs.

```
System Memory Size: 4.0 GB, System Memory Speed: 800 MHz, Voltage: 1.5V


Broadcom NetXtreme II Ethernet Boot Agent v5.2.7
Copyright (C) 2000-2009 Broadcom Corporation
All rights reserved.
Press Ctrl-S to Configure Device (MAC Address - 0024E867D111)


Adaptec 1225SA SATA HostRAID BIOS V6.0-0 B2328
(c) 1998-2007 Adaptec, Inc. All Rights Reserved.

◄◄◄ Press <Ctrl><A> for Adaptec RAID Configuration Utility! ►►►

Controller #00: Adaptec 1225SA at PCI Bus:03, Dev:00, Func:00
SerialNumber = 0KX0B0040013
Loading Configuration...
00:00 WDC WD20EADS-00R6B0 01.00A01     1.81 TB Healthy     3.0 Gb/s

SATA JBOD- PORT-0   WDC WD20EADS-00R     1.81 TB     Legacy

1 JBOD Device(s) Found.

_
```

Abb. 5.28: Meldung eines optionalen ROMs beim Booten

In den Anfangszeiten des PCs gab es alle möglichen Arten von Komponenten mit zusätzlichem ROM. Das optionale ROM wurde inzwischen aber weitgehend durch flexiblere Verfahren abgelöst, wie z.B. die im nächsten Abschnitt vorgestellten Gerätetreiber. Eine wichtige Ausnahme stellen dabei Grafikkarten dar. Alle heute hergestellten Grafikkarten besitzen ihr eigenes BIOS. Optionales ROM funktioniert tadellos, lässt sich aber nur schwer aktualisieren. Aus diesem Grund verwenden die meisten Hardwarekomponenten im PC Software für das eigene BIOS.

5.3.2 Gerätetreiber

Bei einem *Gerätetreiber* handelt es sich um nichts anderes als um auf Datenträgern gespeicherte Dateien, die alle Befehle enthalten, die für die Kommunikation mit der jeweiligen Komponente benötigt werden, für die der Treiber geschrieben wurde. Alle Betriebssysteme kennen Verfahren, um Gerä-

tetreiber beim Booten des Systems in den Arbeitsspeicher zu laden. Welche Gerätetreiber installiert werden müssen, entnimmt das Betriebssystem bestimmten Dateien, die Listen der vom System beim Booten benötigten Gerätetreiber enthalten. Alle Betriebssysteme können derartige Listen am Anfang des Bootprozesses auswerten und die darin aufgeführten Dateien in den Arbeitsspeicher laden. Die CPU (und das Betriebssystem) kann dann nachfolgend mit der vom Gerätetreiber jeweils unterstützten Hardware kommunizieren.

Gerätetreiber werden beim Kauf zusammen mit dem Gerät ausgeliefert. Wenn Sie beispielsweise eine Soundkarte oder einen Monitor kaufen, liegt dem Gerät irgendein Medium bei, meist eine CD-ROM, das die benötigten Gerätetreiber (und oft einer Reihe zusätzlicher Programme) enthält. Allgemein werden diese Datenträger *Installations-CD* genannt (Abbildung 5.29).

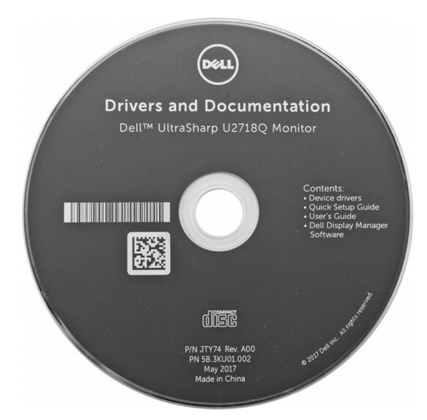


Abb. 5.29: Installations-CD für einen Monitor

Oftmals möchte man die Installationsmedien nicht verwenden und die Sache lieber dem Betriebssystem überlassen. Alle Betriebssysteme bieten die Möglichkeit, online nach Gerätetreibern zu suchen und diese zu installieren. Es gibt Situationen, in denen Sie Gerätetreiber manuell hinzufügen oder entfernen müssen. Windows verwendet eine spezielle Datenbank, die *Registry* (*Registrierungsdatenbank*), in der alle wichtigen Daten des Systems abgelegt sind, einschließlich der Gerätetreiber. In Kapitel 12 werden wir uns die Registry ausführlich ansehen. Um diese Treiber einzurichten, sollten Sie nicht direkt auf die Registry zugreifen, sondern dazu den in Kapitel 2 erwähnten Geräte-Manager verwenden.

5.3.3 BIOS überall!

Mittlerweile wissen Sie, dass alle Hardwarekomponenten im System auf Programme angewiesen sind, die der CPU den erforderlichen Code zur Kommunikation mit ihnen zur Verfügung stellen. Der Code kann sich im System-ROM auf dem Mainboard, im ROM auf der Komponente oder auch auf der Festplatte in einer Datei befinden, die beim Booten in den Arbeitsspeicher geladen wird. Überall im System begegnet man dem BIOS. Sie werden sich gelegentlich immer wieder einmal damit befassen müssen.

5.4 POST (Power-On Self Test)

Das BIOS ist nicht das einzige Programm im System-ROM. Wenn der Computer eingeschaltet oder ein Reset durchgeführt wird, startet er ein spezielles Programm, das ebenfalls im ROM-Chip gespeichert ist und das *POST* (*Power-On Self Test*) (*Einschalt-Selbsttest*) genannt wird. Der POST prüft bei jedem Bootvorgang das System. Er fordert im Rahmen dieses Tests über einen Standardbefehl alle Komponenten dazu auf, sich selbst zu prüfen. Daraufhin führen alle angesprochenen PC-Komponen-

ten ihre eigenen, internen Diagnoseroutinen aus. Der POST selbst teilt den Komponenten nicht mit, was diese prüfen sollen. Wie gut oder ausführlich die Diagnoseroutinen sind, bleibt den Entwicklern der jeweiligen Komponenten überlassen.

Betrachten wir den POST ein wenig genauer. Nehmen wir an, irgendein Gerät, wie beispielsweise der Tastatur-Controller, führt seine Diagnoseroutinen aus und stellt eine Fehlfunktion fest. Was kann der POST dann machen? Eigentlich nur eins, nämlich sie dem Benutzer des Rechners melden! Und wie macht er das? Dazu hat er zwei Möglichkeiten, nämlich über akustische Signale (Pieptöne) oder mittels Textmeldungen auf dem Bildschirm.

5.4.1 Vor und während des Grafikkartentests: Die Piepcodes

Der Computer testet zuerst die grundlegenden Systemkomponenten bis hin zur Grafikkarte. In den alten PCs hörte man eine Folge von Pieptönen – auch als *Beep-Codes* bezeichnet –, wenn irgendetwas nicht in Ordnung war. Über die Pieptöne vor und während des Tests der Grafikkarte konnte der Computer mit Ihnen kommunizieren. (Wenn ein POST-Fehler auftritt, bevor die Grafikkarte verfügbar ist, muss man Pieptöne verwenden, weil natürlich noch kein Text ausgegeben werden kann.) Die Bedeutung der dabei ertönenden Pieptöne war vom jeweiligen BIOS-Hersteller abhängig. Die Bedeutung der Pieptöne des Mainboards wurde dabei üblicherweise in dessen Handbuch beschrieben.

Bei den meisten modernen PCs gibt es nur noch zwei Piepcodes. Einer davon signalisiert eine defekte oder nicht richtig sitzende Grafikkarte (ein langer Ton gefolgt von zwei oder drei kurzen). Der andere weist auf defektes oder fehlendes RAM hin (ein Ton, der unbegrenzt wiederholt wird).

Vorsicht

Es gibt im Internet zwar viele Informationen über Pieptöne, aber sie sind meist hoffnungslos veraltet!

Auf den meisten anderen PCs hört man drei weitere Tonfolgen (obwohl es sich dabei nicht um offizielle Beep-Codes handelt). Nach einem erfolgreichen POST erzeugt der PC einen oder zwei kurze Pieptöne, die Sie einfach darüber informieren sollen, dass alles funktioniert. Die meisten Systeme machen einen befremdlichen Lärm, wenn RAM fehlt oder schwer beschädigt ist. Anders als traditionelle Beep-Codes wird dieser Code wiederholt, bis Sie das System ausschalten. Darüber hinaus kann Ihr Lautsprecher Pieptöne ausgeben, die nicht zum POST oder überhaupt zum Booten gehören. Einer der gebräuchlicheren ist eine Folge von Pieptönen, nachdem das System eine Zeit lang gelaufen ist. Dabei handelt es sich meist um ein Alarmsignal, das darauf hinweisen soll, dass die CPU zu heiß geworden ist.

5.4.2 Fehlermeldungen als Text

Nach erfolgreichem Test der Grafikkarte werden alle POST-Fehlermeldungen auf dem Bildschirm angezeigt. Wenn Textfehlermeldungen angezeigt werden, dann sind diese meist (aber nicht immer) selbsterklärend (Abbildung 5.30). Textmeldungen sind viel aussagekräftiger, da Sie auf dem Bildschirm nachlesen können, welche Komponenten defekt sind.

```
                                                   F10 = System Services
                                                 F11 = BIOS Boot Manager
Keyboard failure                                        F12 = PXE Boot

One 1.86 GHz Dual-core Processor, Bus Speed:4.80 GT/s, L2/L3 Cache:512 KB/4 MB
System running at 1.86 GHz
System Memory Size: 4.0 GB, System Memory Speed: 800 MHz, Voltage: 1.5V
```

Abb. 5.30: Eine Textfehlermeldung

5.4.3 POST-Karten

Pieptöne, numerische Codes und Textfehlercodes können hilfreich sein, aber manchmal auch in die Irre führen. Schlimmer noch: Es gibt manche defekte Geräte, die den POST unterbrechen und die Maschine in eine Endlosschleife laufen lassen. Der PC scheint dadurch komplett »tot« zu sein, piepst nicht einmal und zeigt auch nichts auf dem Bildschirm an. In diesem Fall benötigen Sie Hilfsmittel zur Überwachung des Selbsttests und zur Anzeige der Fehlerursache. Solche Geräte sind unter der Bezeichnung *POST-Karten* bekannt.

POST-Karten sind einfache Steckkarten, die in einen Erweiterungssteckplatz des Systems installiert werden. Alle POST-Karten verfügen über eine kleine zweistellige LED-Anzeige, die über das vom POST gerade getestete Gerät informiert (Abbildung 5.31).

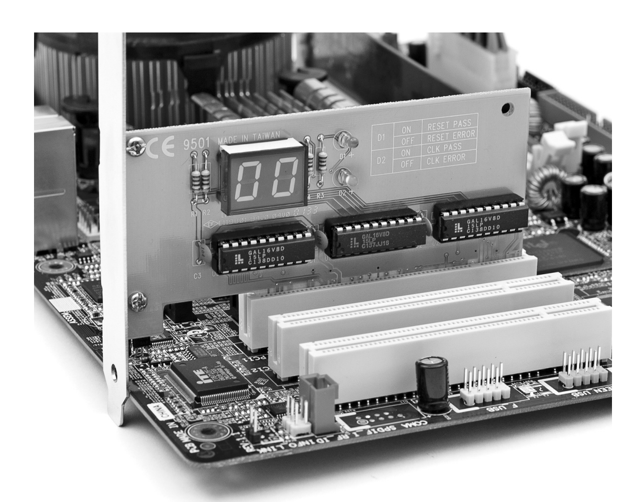


Abb. 5.31: POST-Karte bei der Arbeit

POST-Karten waren lange ein unerlässliches Hilfsmittel für Techniker, heutzutage verwende ich sie allerdings nur, wenn mir ein scheinbar »toter« PC begegnet, um festzustellen, auf welcher Ebene das Gerät »tot« ist. Wenn die POST-Karte nichts anzeigt, weiß ich, dass das Problem vor dem POST auftritt und entweder Netzteil, CPU, RAM oder Mainboard betrifft. Gibt es hingegen eine Anzeige, weist das darauf hin, dass ich auch andere Dinge prüfen muss, wie etwa die Festplatten usw.

5.4.4 Der Bootprozess

Bei allen Personal Computern muss es einen Vorgang geben, der ihnen die Betriebsaufnahme ermöglicht. Wenn der Rechner erst einmal mit Strom versorgt wird, dann sorgen Hardware, Firmware und Software in enger Zusammenarbeit dafür, dass sich der PC selbst startet bzw. bootet.

Sobald das Netzteil nach dem Einschalten die richtige Spannung liefert, liest die CPU eine spezielle Leitung namens *Power Good*. Sobald an dieser Leitung eine gewisse Spannung anliegt, weiß die CPU, dass das System über genügend Energie zum Start des Bootvorgangs verfügt. Alle Intel- und geklonten CPUs verfügen über eine eingebaute Speicheradresse, die in dem Moment über den Adressbus übertragen wird, in dem die CPU über die Leitung Power Good aufgeweckt wurde. Diese spezielle Adresse ist bei allen CPUs vom ältesten 8086er bis hin zum neuesten Mikroprozessor dieselbe, und sie verweist auf die erste Zeile des POST-Programms im System-ROM! Auf diese Weise startet das System den POST. Nach Beendigung des POSTs muss der Computer noch über Mittel und Wege verfügen, die Programme auf der Festplatte ausfindig zu machen, um das Betriebssystem laden zu können. Was danach geschieht, unterscheidet sich zwischen dem alten BIOS und dem neuen UEFI.

In älteren BIOS-Umgebungen übergibt der POST die Kontrolle an die letzte BIOS-Funktion, den *Bootstrap-Loader*. Dieser besteht aus kaum mehr als einigen Dutzend Zeilen BIOS-Code, die an das Ende des POST-Programms angehängt sind. Seine Aufgabe besteht in der Suche nach dem Betriebssystem. Der Bootstrap-Loader liest CMOS-Information, um festzustellen, wo er zuerst nach einem Betriebssystem suchen soll. Das CMOS-Setup-Programm Ihres PCs bietet eine Option, die Sie konfigurieren, um dem Bootstrap-Loader mitzuteilen, auf welchen Geräten er nach einem Betriebssystem suchen soll und in welcher Reihenfolge er diese durchsuchen soll. Hierbei handelt es sich um die *Bootreihenfolge* (Abbildung 5.32).

```
▶ Hard Disk Book Priority    [Press Enter]
  First Boot Device          [CDROM]
  Second Boot Device         [Hard Disk]
  Third Boot Device          [CDROM]
```

Abb. 5.32: Die CMOS-Bootreihenfolge

Fast alle Speichergeräte – Festplatten, SSD-Laufwerke, CDs, DVDs und sogar USB-Sticks – können für das Booten eines Betriebssystems vorbereitet werden. Dazu wird ein spezieller Speicherbereich darauf angelegt, der *Bootsektor* oder *Startsektor* genannt wird. Wenn das Gerät bootfähig ist, enthält sein Startsektor ein spezielles Programm, das dem System mitteilt, wo sich das Betriebssystem befindet. Ein Gerät mit funktionalem Betriebssystem wird *bootfähiger Datenträger* oder *Systemdatenträger* genannt. Wenn der Bootstrap-Loader einen funktionierenden Startsektor findet, übergibt er die Kontrolle an das Betriebssystem und entfernt sich selbst aus dem Speicher. Findet er keinen Startsektor, fährt er mit dem nächsten Gerät in der im CMOS-Setup angegebenen Bootreihenfolge fort. Die Bootreihenfolge ist für Techniker wichtig, weil sie durch sie spezielle bootfähige Geräte einbauen können, von denen sie Dienstprogramme zur Rechnerwartung ausführen können, ohne dabei auf das primäre Betriebssystem angewiesen zu sein.

Bei UEFI-Systemen übergibt der POST die Kontrolle an den Bootmanager, der die Bootkonfiguration überprüft und den Boot-Loader zum Laden des Betriebssystems direkt lädt (Abbildung 5.33). Ein Startsektor wird nicht mehr benötigt. Bootmanager und Bootkonfiguration werden in der UEFI-Firmware gespeichert.

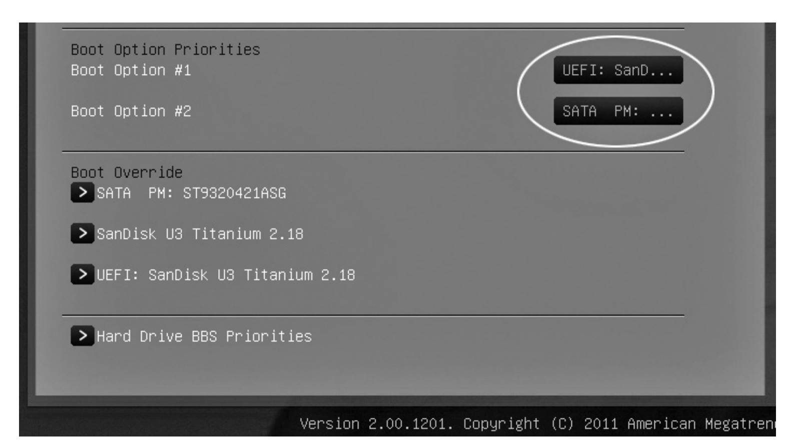


Abb. 5.33: UEFI-Bootmodus und die Optionen des Bootmanagers

Hinweis

Wenn Sie eine für ein BIOS eingerichtete bootfähige Festplatte in ein UEFI-System einbauen, wird das System höchstwahrscheinlich auf den BIOS-Kompatibilitätsmodus zurückschalten und wie gewohnt starten. Mehr zu diesem Thema finden Sie in Kapitel 9, *Vorbereitung und Wartung von Festplatten.*

Bei einigen BIOS-Versionen kann man eine spezielle Umgebung namens *PXE* (*Preboot Execution Environment*) aktivieren. Der PC kann nun starten, ohne auf lokalen Speicher zugreifen zu müssen, indem er via Netzwerk ein auf einem Server befindliches Betriebssystem lädt. Sie werden in Kapitel 11 mehr darüber erfahren, wenn es um das Thema Windows-Installation geht.

5.5 Wartung von BIOS/UEFI und CMOS

Mit dem Thema BIOS und CMOS werden Sie sich nicht allzu häufig befassen müssen. Das eigentliche BIOS ist unsichtbar. Der einzige Hinweis auf seine Existenz ist der POST. Das CMOS-Setup macht sich hingegen beim Starten deutlich bemerkbar. Das CMOS-Setup funktioniert heute meist problemlos, ohne dass man sich je weiter darum kümmern müsste. Ambitionierte Techniker rufen aber gelegentlich das CMOS-Setup auf und nehmen dort Änderungen vor. Und hier treten dann meistens die Probleme auf.

Wenn Sie sich im CMOS-Setup zu schaffen machen, nehmen Sie immer nur so viele Änderungen auf einmal vor, wie Sie sich merken können. Notieren Sie sich die ursprünglichen Einstellungen oder schießen Sie ein Foto davon. Auf diese Weise können Sie gegebenenfalls alles wieder rückgängig machen. Ändern Sie keine Einstellungen, von denen Sie nicht genau wissen, was sie bewirken! Man kann Computer sogar ernsthaft beschädigen, wenn man mit CMOS-Einstellungen spielt, die man nicht versteht.

5.5.1 Standardeinstellungen und optimierte Einstellungen

Bei allen CMOS-Setup-Programmen gibt es verschiedene Optionen zum Zurücksetzen, die üblicherweise als Standardeinstellungen (*Default Settings*) und für das Betriebssystem optimierte Einstellungen (*OS Optimized Defaults*) bezeichnet werden (Abbildung 5.34). Auf diese Weise brauchen Sie sich nicht alle diese merkwürdigen Einstellungen zu merken, die Sie ohnehin nie ändern. Die narrensicheren Standardeinstellungen setzen alles auf die einfachsten Werte zurück. Manchmal hilft es, diese Einstellungen zu verwenden, wenn es zu offenbar sehr systemnahen Fehlern wie Abstürzen kommt, die sich durch eigentlich plausiblere Maßnahmen nicht beheben lassen. Die optimierten Einstellungen sorgen für die bestmögliche Stabilität und Geschwindigkeit des Systems. Verwenden Sie diese Option, wenn Sie mit den CMOS-Einstellungen »herumgespielt« haben und alles wieder rückgängig machen möchten.

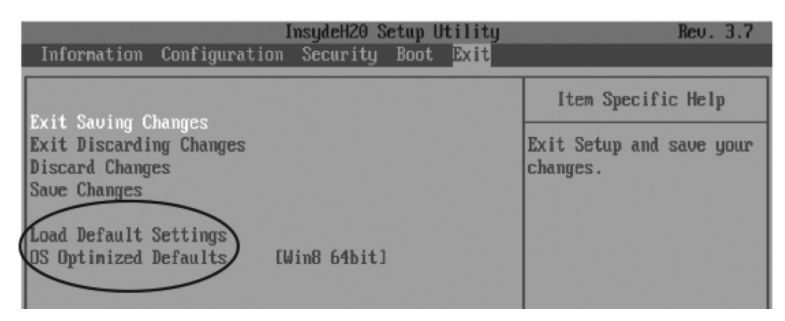


Abb. 5.34: Optionen zum Zurücksetzen des CMOS

5.5.2 Löschen der CMOS-Einstellungen

In Kapitel 3 haben Sie bereits erfahren, wie man die CMOS-Einstellungen löschen kann, es lohnt aber, den Vorgang kurz zu rekapitulieren. Wenn Sie irgendeine fehlerhafte Einstellung vorgenommen haben (etwa eine zu hohe Übertaktung oder die Deaktivierung einer unverzichtbaren Funktion), die dazu führt, dass der Rechner unbrauchbar ist, können Sie das CMOS auf die Werkseinstellungen zurücksetzen und wieder von vorne anfangen.

Nahezu alle Mainboards besitzen einen Jumper (oder einen vergleichbaren Mechanismus), der als *CMOS-Clear* oder *CLRTC* bezeichnet wird (Abbildung 5.35), über den die CMOS-Standardeinstellungen wiederhergestellt werden können.

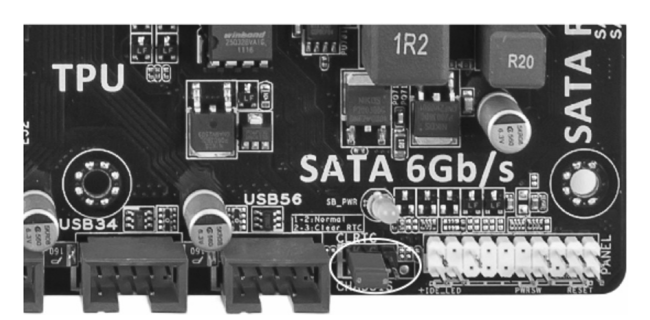


Abb. 5.35: CMOS-Clear-Jumper

Zum Löschen der CMOS-Einstellungen müssen Sie den PC ausschalten und vom Stromnetz trennen. Öffnen Sie das Gehäuse und suchen Sie nach dem CMOS-Clear-Jumper. Stecken Sie dann den *Shunt* (die kleine Plastik-Steckbrücke) von den Kontakten 1 und 2 auf die Kontakte 2 und 3 um (Abbildung 5.36). Warten Sie zehn Sekunden und bewegen Sie dann die Steckbrücke wieder in ihre Standardposition. Schließen Sie den Rechner nun wieder ans Stromnetz an und starten Sie das System.

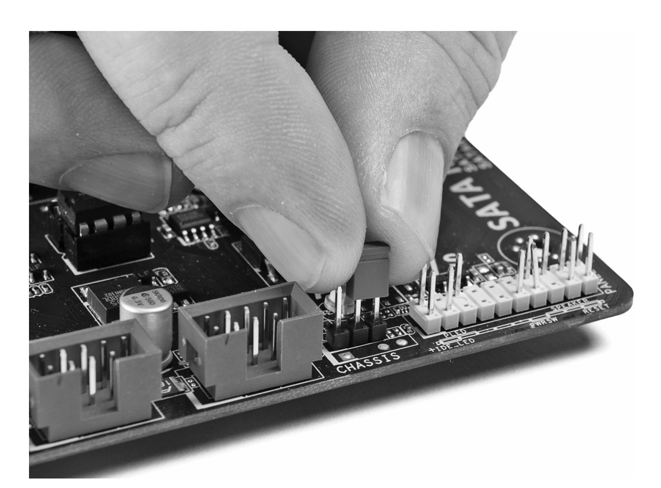


Abb. 5.36: Umstecken des Jumpers zum Löschen der CMOS-Einstellungen

Hinweis

Für hinsichtlich des Übertaktens besonders experimentierfreudige Anwender gibt es spezielle Mainboards, die einen eigenen eingebauten Taster zum Zurücksetzen des CMOS besitzen. Das nenne ich Service!

Wenn diese Vorgehensweise nicht zum Erfolg führt oder Sie eines der wirklich seltenen Mainboards ohne CMOS-Clear-Jumper verwenden, können Sie Folgendes tun: Schalten Sie den Rechner aus und trennen Sie ihn vom Stromnetz. Entfernen Sie dann die kleine Knopfzelle (Abbildung 5.37) und warten Sie einige Sekunden. Setzen Sie die Batterie dann wieder ein und starten Sie den Rechner neu.

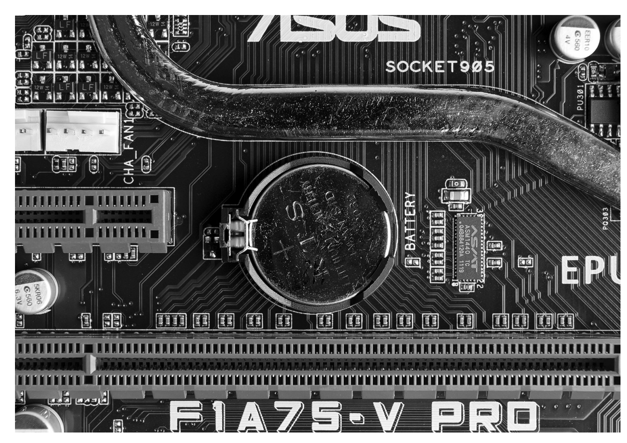


Abb. 5.37: Eine CMOS-Batterie

5.5.3 Verlust der CMOS-Einstellungen

Das CMOS braucht immer ein wenig Spannung für die Echtzeituhr und um seine Daten nicht zu vergessen. Auf den Mainboards befindet sich deshalb eine Batterie, heute meist eine 3-Volt-Knopfzelle, die das CMOS-RAM mit der erforderlichen Spannung versorgt, während der Computer ausgeschaltet ist (siehe Abbildung 5.37). Typische Systeme verwenden eine Batterie des Typs CR2032. (Welchen Typ verwendet Ihr System?)

Wenn die Batterie leer ist, gehen alle CMOS-Daten verloren. Wenn die Daten des CMOS-Chips versehentlich gelöscht werden, bootet der PC möglicherweise nicht mehr, oder Sie erhalten beim Booten übel klingende Fehlermeldungen. Jeder nach dem Jahr 2002 hergestellte PC bootet mit den Werkseinstellungen, wenn das CMOS gelöscht wurde, wodurch die Wahrscheinlichkeit, dass er überhaupt nicht bootet, heute eher gering ist. Fehlermeldungen werden beim Booten aber dennoch angezeigt. Nachfolgend einige Beispiele für Fehler, die auf verlorene CMOS-Daten hinweisen:

- CMOS configuration mismatch
- CMOS date/time not set
- BIOS time and settings reset
- No boot device available
- CMOS battery state low

Und nachfolgend einige der häufigsten Ursachen für den Verlust von CMOS-Daten:

- Entfernen und Einsetzen von Steckkarten
- Berührung des Mainboards
- Auf das Mainboard gefallene Gegenstände
- Schmutz auf dem Mainboard
- Defekte Netzteile
- Spannungsspitzen

Wenn Sie es mit einem derartigen Fehler zu tun bekommen oder wenn die Systemuhr bei jedem Systemstart auf den 1. Januar zurückgesetzt wird, dann ist die Batterie auf dem Mainboard schwach geworden und muss ersetzt werden. Dazu schieben Sie die Batteriehalterung mit einem Schraubendreher vorsichtig zurück. Die Batterie sollte nun herausspringen und sich einfach entnehmen lassen. Bevor Sie die neue Batterie einsetzen, überprüfen Sie sicherheitshalber, ob der Batterietyp mit dem der alten Batterie übereinstimmt. Damit die CMOS-Einstellungen während des Batteriewechsels erhalten bleiben, lassen Sie den PC einfach an die Steckdose angeschlossen. Die 5-Volt-Stromversor-

gung der modernen Mainboards sorgt für ausreichend Strom, um das CMOS zu versorgen und die Daten zu erhalten. Natürlich müssen Sie *äußerst* vorsichtig sein, damit es zu keinen elektrostatischen Entladungen kommt, während Sie die Batterie eines laufenden Systems wechseln!

5.6 Flash-ROM aktualisieren

Der Inhalt von Flash-ROM-Chips lässt sich aktualisieren. Wenn Sie das System-BIOS aktualisieren müssen, damit neue Technologien unterstützt werden, führen Sie einfach zusammen mit einer Aktualisierungsdatei ein kleines Befehlszeilenprogramm aus, und schon haben Sie ein neues, aktualisiertes BIOS! Man bezeichnet diesen Vorgang als *Firmwareaktualisierung*. Die BIOS-Hersteller verwenden leicht unterschiedliche Verfahren zur BIOS-Aktualisierung (dem *Flashen* des BIOS), aber im Allgemeinen müssen Sie einen Wechseldatenträger anschließen (meistens einen USB-RAM-Stick), der das aktualisierte BIOS enthält und dann im BIOS-Setup-Programm die Aktualisierung durchführen.

Etliche Mainboard-Hersteller bieten auch Programme für Windows-basierte Flash-ROM-Updates an, die im Internet nach Aktualisierungen suchen und sie zur Installation herunterladen. Mit den meisten dieser Programme können Sie auch die aktuelle BIOS-Version sichern, um bei auftretenden Problemen wieder zu dieser zurückkehren zu können. Ohne eine solche Sicherung könnten Sie ansonsten das Mainboard wegschmeißen müssen, wenn beim Flash-BIOS-Update Fehler auftreten. Legen Sie also immer eine Sicherung an!

Viele Mainboard-Hersteller bieten inzwischen Setup-Programme, die sich direkt mit dem Internet verbinden können, um auf Aktualisierungen zuzugreifen. Abbildung 5.38 zeigt ein solches Programm.

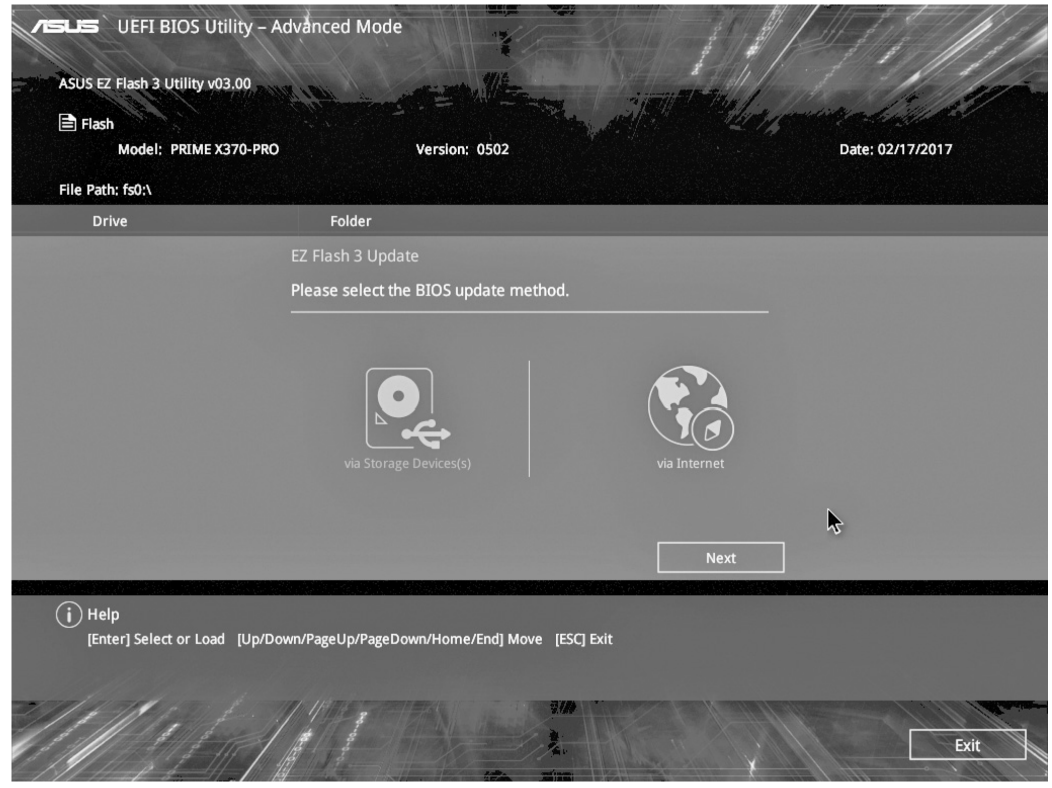


Abb. 5.38: Programm zur CMOS-Aktualisierung eines ASUS-Mainboards

Hinweis

Eine fehlgeschlagene BIOS/UEFI-Aktualisierung kann einen Computer oder ein Gerät unbrauchbar machen.

Zum Abschluss dieses Abschnitts über die BIOS-Aktualisierung noch eine Warnung: Letztlich sollten Sie das BIOS nicht aktualisieren, wenn es keinen wirklich guten Grund dafür gibt. In diesem Fall gilt tatsächlich: Was nicht kaputt ist, muss man auch nicht reparieren!

Wichtig

Techniker sagen meist »BIOS flashen«. Die CompTIA A+-Prüfungen sprechen hingegen von der »Installation einer Firmwareaktualisierung«.

5.7 Wiederholung

5.7.1 Fragen

1. Welche Funktion hat das BIOS für den Computer? (Wählen Sie die beste Antwort aus.)
   A. Das BIOS sorgt für die physische Schnittstelle verschiedener Komponenten, wie z.B. der USB- und FireWire-Anschlüsse.
   B. Das BIOS enthält Programme, die der CPU die Kommunikation mit anderen Hardwarekomponenten erlauben.
   C. Das BIOS stellt den Speicher für Anwendungen zur Verfügung, die von der Festplatte geladen werden.
   D. Das BIOS stellt den Speicher für Anwendungen zur Verfügung, die in das System-RAM geladen werden.
2. Wie lautet die richtige Bootreihenfolge bei einem älteren, mit BIOS arbeitenden PC?
   A. CPU, POST, Power Good, Boot-Loader, Betriebssystem
   B. POST, Power Good, CPU, Boot-Loader, Betriebssystem
   C. Power Good, Boot-Loader, CPU, POST, Betriebssystem
   D. Power Good, CPU, POST, Boot-Loader, Betriebssystem
3. Johanna hat beschlossen, eine zweite Festplatte in ihren Computer einzubauen. Sie glaubt, sie hat sie korrekt eingebaut, sie wird in Windows jedoch nicht angezeigt. Mit welcher der folgenden Maßnahmen kann Johanna am wahrscheinlichsten herausfinden, was zu tun ist, um das Problem zu lösen?
   A. Neustart des Computers und zweimaliges Drücken der F-Taste auf der Tastatur. Damit wird dem Computer signalisiert, dass er über zwei Festplatten verfügt.
   B. Neustart des Systems und auf die Anweisung achten, wie sie in das CMOS-Setup gelangt (z.B. könnte eine Meldung ausgegeben werden, die `Entf`-Taste zu drücken). Danach folgt sie der Anweisung, um das CMOS-Setup aufzurufen.
   C. Sie drückt in Windows zweimal die `Entf`-Taste, um das CMOS-Setup aufzurufen.
   D. Sie wählt unter Windows START|AUSFÜHREN und tippt `hard drive` ein. Dann klickt sie auf OK, um den Assistenten zur Einrichtung von Festplatten zu starten.
4. Herbert hat sich eine neue TV-Karte für seinen Computer gekauft. Beim Auspacken stellt er jedoch fest, dass es keine Treiber-CD gibt, sondern nur eine Anwendungs-CD für die Installation der TV-Software. Nach Installation der Karte und der Software funktioniert alles reibungslos. Welche Erklärung ist am wahrscheinlichsten?

A. Die Komponente benötigt kein BIOS und deshalb auch keine Treiber-CD.

B. Die Komponente besitzt ein optionales ROM, das vom BIOS geladen wird, und benötigt deshalb keine Treiber-CD.

C. Windows unterstützt TV-Karten standardmäßig, deshalb braucht man keine Treiber-CD.

D. Der Hersteller hat einen Fehler gemacht und hat nicht alles geliefert, was man für das Gerät benötigt.

5. Wodurch wird die Beziehung zwischen Hardware und BIOS am besten beschrieben?

A. Alle Hardwarekomponenten benötigen ein BIOS.

B. Alle an das Mainboard über Flachbandkabel angeschlossenen Hardwarekomponenten benötigen ein BIOS.

C. Alle in das Mainboard integrierten Komponenten benötigen ein BIOS.

D. Einige Hardwarekomponenten benötigen ein BIOS.

6. Nach einem plötzlichen Stromausfall wurde der PC von Timo neu gestartet, aber auf dem Bildschirm wird nichts angezeigt. Der PC piept nur noch unaufhörlich. Welche Ursache ist am wahrscheinlichsten?

A. Der Stromausfall hat das RAM gegrillt.

B. Der Stromausfall hat die Grafikkarte getoastet.

C. Der Stromausfall hat die Festplatte geröstet.

D. Der Stromausfall hat die CPU zerstört.

7. Dieter stellt fest, dass ein verärgerter früherer Angestellter bei seiner Kündigung den Computer sabotieren wollte und im CMOS ein Passwort eingerichtet hat, sodass der Computer nicht mehr bootet. Wie kann Dieter das Problem lösen?

A. Dieter sollte den Computer booten und dabei die linke [⇧]-Taste gedrückt halten. Dadurch werden die CMOS-Daten gelöscht.

B. Dieter sollte verschiedene Kombinationen des Namens des früheren Angestellten ausprobieren. Die meisten Leute verwenden ihren Namen oder ihre Initialen als CMOS-Passwörter.

C. Dieter sollte den Jumper für das Löschen des CMOS auf dem Mainboard suchen. Anschließend kann er den Kontakt mit einem Jumper schließen und den Computer neu starten, um die CMOS-Daten zu löschen.

D. Dieter muss sich ein neues Mainboard zulegen. Wenn er das CMOS-Passwort nicht kennt, kann er nichts machen.

8. Richard aus der Verkaufsabteilung hat an seinem CMOS herumgefummelt und verschiedene Änderungen vorgenommen, mit denen er seinen PC optimieren wollte. Der funktioniert jetzt aber nicht mehr richtig. Er kann booten, kommt aber nur noch ins CMOS-Setup. Windows startet nicht mehr. Mit welcher Auskunft eines Technikers kann er sein System am ehesten wieder zum Laufen bringen?

A. Starten Sie den Computer etwa dreimal neu. Auf diese Weise wird das CMOS gelöscht und der Computer läuft wieder.

B. Öffnen Sie den Computer und suchen Sie den Jumper für das Löschen des CMOS. Entfernen Sie irgendwo auf dem Mainboard eine Steckbrücke und schließen Sie mit ihr den Kontakt zum Löschen des CMOS. Booten Sie neu und setzen Sie die Steckbrücke dann wieder dort auf, wo Sie diese entfernt haben. Booten Sie neu. Jetzt sollte alles wieder funktionieren.

C. Rufen Sie das CMOS-Setup auf und suchen Sie die Option zum Laden eines Plug&Play-Betriebssystems. Stellen Sie sicher, dass sie aktiviert ist. Speichern Sie die Einstellungen und verlassen Sie das CMOS. Starten Sie Windows wie üblich. Jetzt sollte wieder alles funktionieren.

D. Rufen Sie das CMOS-Setup auf und suchen Sie die Option zum Laden der OPTIMIZED DEFAULT-Einstellungen. Speichern Sie die Einstellungen und verlassen Sie das CMOS. Starten Sie Windows wie üblich. Jetzt sollte alles wieder funktionieren.

9. Tina bootet ein älteres Pentium-System, über das sich mehrere Benutzer im Büro beschwert haben. Das System startet und beginnt mit dem POST, bricht diesen aber ab. Der Bildschirm zeigt die Meldung »CMOS configuration mismatch« an. Was ist die wahrscheinlichste Ursache für diesen Fehler?
   A. Schwache CMOS-Batterie
   B. Defekte CPU
   C. Defektes RAM
   D. Beschädigtes System-BIOS
10. Wo speichert Windows Angaben zu Gerätetreibern?
   A. COMPUTER
   B. HARDWARE
   C. Registry
   D. TREIBER UND EINSTELLUNGEN

5.7.2 Antworten

1. **B.** Das BIOS stellt die Programme bereit, mit deren Hilfe die CPU mit anderen Hardwarekomponenten kommunizieren kann.
2. **D.** Die korrekte Boot-Reihenfolge lautet: Power Good, CPU, POST, Boot-Loader, Betriebssystem.
3. **B.** Johanna sollte den Computer neu starten und auf Anweisungen achten, wie sie in das CMOS-Setup gelangt (z.B. könnte eine Meldung sie dazu auffordern, die `Entf`-Taste zu drücken). Anschließend sollte sie der Anweisung folgen, um in das CMOS-Setup zu gelangen.
4. **B.** Da das Gerät funktioniert, besitzt es sehr wahrscheinlich ein optionales ROM.
5. **A.** Alle Hardwarekomponenten benötigen ein BIOS!
6. **A.** Das wiederholte Piepen und der nicht funktionierende PC weisen auf ein Problem mit dem RAM hin.
7. **C.** Dieter sollte den Jumper für das Löschen des CMOS auf dem Mainboard suchen. Anschließend sollte er den Kontakt schließen und den Computer neu starten, um die CMOS-Daten zu löschen.
8. **D.** Geben Sie Richard bloß keinen Schraubendreher! Er soll die OPTIMIZED DEFAULT-Einstellungen laden, das sollte funktionieren.
9. **A.** Wahrscheinlich ist die CMOS-Batterie zu schwach.
10. **C.** Windows speichert Angaben zu Gerätetreibern in der Registry.

Mainboards 6

Themen in diesem Kapitel:

- Funktionsweise von Mainboards
- Erweiterungsmöglichkeiten durch Steckkarten
- Mainboards aufrüsten und installieren
- Fehlersuche bei Problemen mit dem Mainboard

Das *Mainboard* bildet die Basis des Personal Computers. Alle Hardwarekomponenten von der CPU bis hin zur einfachsten Erweiterungskarte sind direkt oder indirekt mit dem Mainboard verbunden. Das Mainboard enthält alle Leitungen – sogenannte *Leiterbahnen* –, die die verschiedenen Busse des Systems darstellen. Es enthält die meisten der von Peripheriegeräten verwendeten Anschlüsse und verteilt den Strom des Netzteils (Abbildung 6.1). Ohne Mainboard hätten Sie buchstäblich keinen PC.

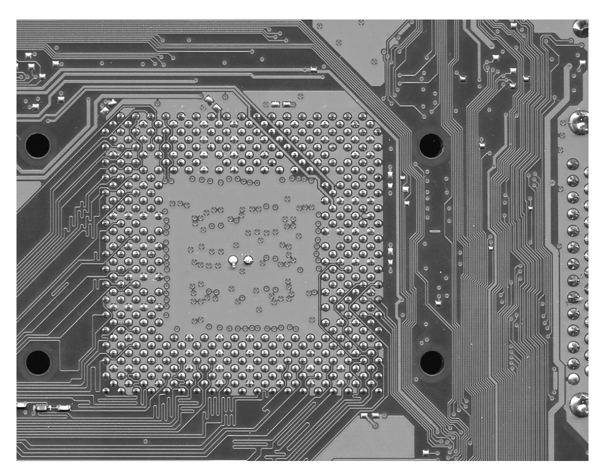


Abb. 6.1: Sichtbare Leiterbahnen unterhalb des CPU-Sockels auf einem Mainboard

In diesem Kapitel wird zunächst erklärt, wie ein Mainboard funktioniert, wobei die verschiedenen Formfaktoren zur Sprache kommen und was diese voneinander unterscheidet. Im zweiten Abschnitt untersuchen wir die Erweiterungsmöglichkeiten von Mainboards, und hier insbesondere solche Erweiterungskarten, denen Sie im Alltag begegnen werden und wie man diese installiert. Der dritte Abschnitt schließlich erläutert Schritt für Schritt die praktische Installation und Aufrüstung von Mainboards. Am Ende des Kapitels gibt es einige Tipps zur Fehlerbehebung bei Mainboards.

Hinweis

Bei modernen Mainboards handelt es sich um mehrschichtige *Leiterplatten* oder auch *gedruckte Schaltungen* (PCB – Printed Circuit Board), die als Träger für elektronische Bauteile dienen. Sie bestehen aus einem elektrisch isolierenden Material (üblicherweise faserverstärkte Kunststoffe wie Epoxidharz). Die darauf befindlichen Leiterbahnen werden aus einer dünnen Kupferschicht herausgeätzt. Dadurch, dass es mehrere Lagen gibt, wirken die Leiterbahnen weniger kompliziert, als sie es tatsächlich sind. Einige der Leiterbahnen sind sichtbar, jedoch besteht jedes Mainboard aus mindestens vier solcher Schichten. Auf diesen Leiterbahnen bewegen sich die Daten und Befehle hin und her, die zwischen CPU, RAM und Peripheriegeräten ausgetauscht werden. Die mehrschichtige Struktur ermöglicht es, auf mehreren Leiterbahnen

gleichzeitig Daten zu übertragen, ohne dass die einzelnen Signale einander in die Quere kommen. Außerdem erlaubt die Mehrschichtigkeit den Herstellern, zusätzliche Elemente und Komponenten in die Mainboards zu integrieren, ohne die Ausmaße der Leiterplatte vergrößern zu müssen. Kürzere Leiterbahnen sind außerdem aufgrund schnellerer Signallaufzeiten von Vorteil. Und schließlich wird ein Mainboard durch mehrere Schichten auch physisch stabiler und lässt sich nicht so leicht verbiegen.

Geschichte und Konzepte

6.1 Wie Mainboards funktionieren

Drei variable und voneinander abhängige Merkmale definieren moderne Mainboards: Formfaktor, Chipsatz und Komponenten. Der *Formfaktor* bestimmt die physischen Abmessungen des Mainboards sowie die allgemeine Anordnung von Komponenten und Anschlüssen. Der *Chipsatz* bestimmt, welcher Prozessortyp und welche Art von Speichermodulen verwendet werden können, und zum Teil auch, welche integrierten Komponenten (auch Erweiterungssteckplätze) von einem Mainboard unterstützt werden. Und schließlich bestimmen die *integrierten Komponenten* die grundlegende Funktionalität des Systems.

Fast alle in Desktops verwendeten Chipsätze stammen entweder von Intel oder AMD. Dass die beiden größten Hersteller von CPUs für Windows, macOS und Linux-basierte Rechner auch die unverzichtbaren dazugehörigen Chipsätze liefern, erscheint daher angemessen.

Jeder gute Techniker sollte Kunden eine Empfehlung hinsichtlich des Mainboards einfach anhand der Spezifikationen geben können. Da das Mainboard die Funktion, Erweiterbarkeit und Stabilität des gesamten Rechners bestimmt, ist es wichtig, dass Sie über Mainboards Bescheid wissen!

Wichtig

Punkt 3.5 der Lernziele der CompTIA A+-Prüfung 1001 konzentriert sich insbesondere auf Mainboards, die sich in klassischen Windows- und Linux-basierten Desktop-PCs finden. Diese Art Mainboard gestattet es Technikern, beispielsweise bestimmte Komponenten auf- oder nachzurüsten. Daher wird in diesem Kapitel durchweg der Begriff »PC« benutzt. Formfaktoren

Formfaktoren sind von der Industrie standardisierte Formvorgaben und Layouts, durch die Mainboards, Gehäuse und Netzteile zusammenpassen und miteinander kombinierbar werden. Ein einzelner Formfaktor gilt für alle drei Komponenten. Beispielsweise haben alle Mainboards eine rechteckige oder quadratische Form, variieren aber im Hinblick auf Gesamtgröße und Layout der eingebauten Komponenten (Abbildung 6.2). Sie müssen ein Mainboard in ein passendes Gehäuse einbauen, damit Anschlüsse und Gehäuseaussparungen an der Rückseite zueinanderpassen.

Die Anschlüsse von Netzteil und Mainboard müssen zueinanderpassen, wobei unterschiedliche Formfaktoren verschiedene Anschlussvarianten besitzen. Der Formfaktor bezieht sich auf Gehäuse, Mainboard und Netzteil, die drei Rechnerkomponenten, die die Luftzirkulation im PC maßgeblich beeinflussen. Letztlich ist der Formfaktor damit auch für die Lüftung des Gehäuses entscheidend.

Um das Mainboard aufrüsten oder Kunden fundierte Empfehlungen geben zu können, müssen Techniker die Formfaktoren kennen. Die PC-Industrie hat im Laufe der Jahre mehrere Formfaktoren definiert (und wieder verworfen), die z.B. AT, ATX und ITX genannt wurden. Wir beginnen mit AT und damit mit dem Urahn aller PC-Formfaktoren.

Hinweis

Falls Sie neugierig geworden sind: Ja, die Buchstaben der Bezeichnungen stehen für bestimmte Wörter. AT bedeutet *Advanced Technology*, ATX *Advanced Technology Extended* und ITX *Information Technology Extended*. Aber kein Mensch verwendet diese Bezeichnungen. Verwenden Sie die Abkürzung.



Abb. 6.2: Typisches Mainboard

AT-Formfaktor

Der AT-Formfaktor (Abbildung 6.3), den IBM Anfang der 1980er-Jahre erfand, war bis Mitte der 1990er-Jahre bei Mainboards vorherrschend. Heute ist AT veraltet.

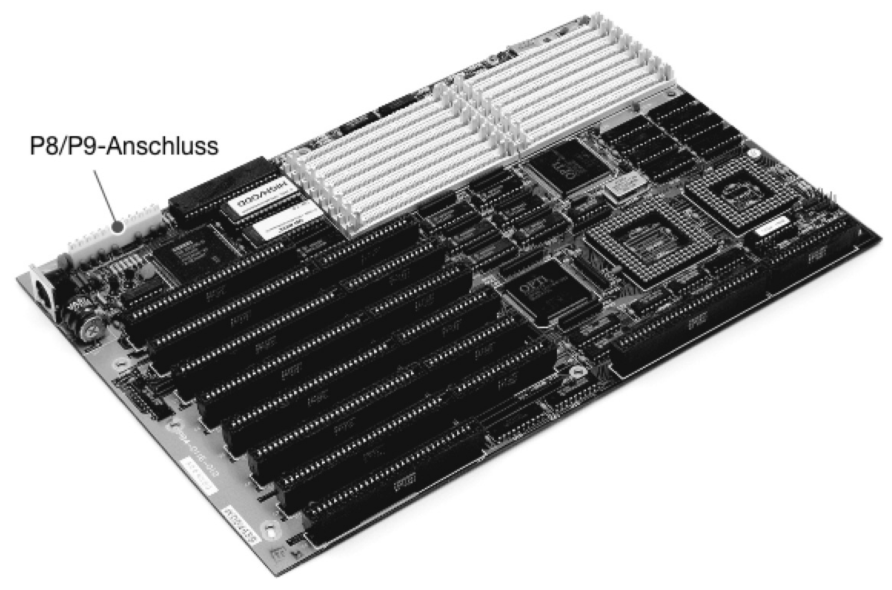


Abb. 6.3: AT-Mainboard

Beim AT-Mainboard gab es einige Größenvarianten, sie waren aber durchweg vergleichsweise groß (Abbildung 6.4). Das Original-AT-Mainboard war riesig, gut 30 cm breit und etwa 33 cm lang. Die PC-Technologie war noch neu und die verschiedenen Chips, die man für den Betrieb der verschiedenen PC-Komponenten benötigte, nahmen noch viel Platz in Anspruch.

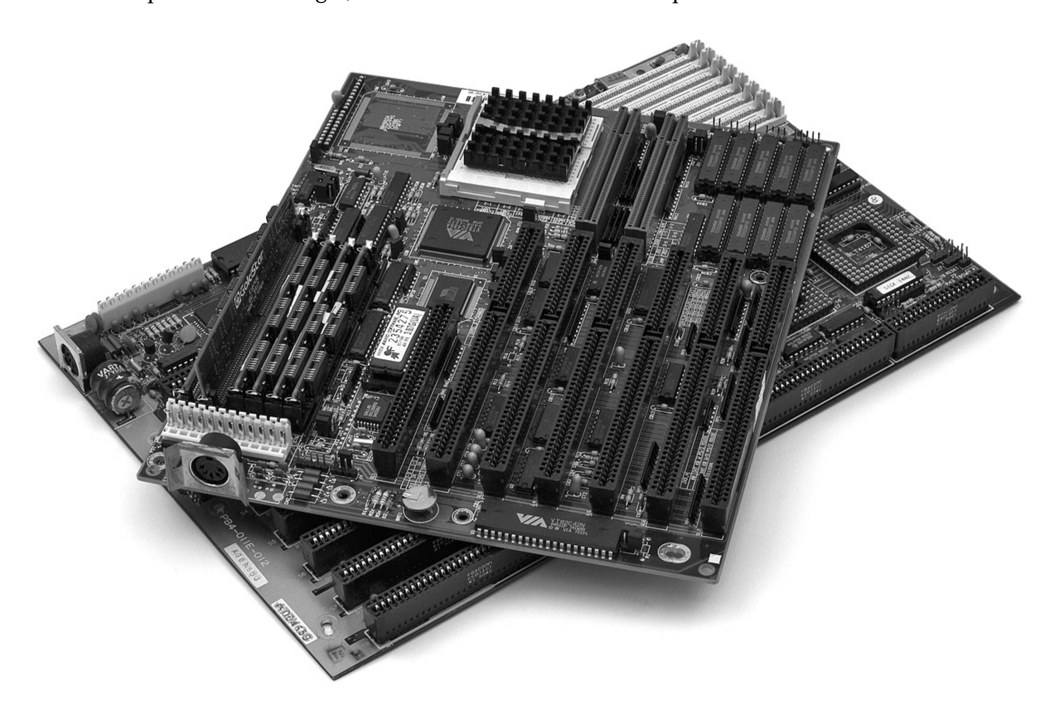


Abb. 6.4: AT-Mainboard (unten) und Baby AT-Mainboard (oben)

Das größte Problem bei AT-Mainboards war, dass es keine externen Anschlüsse gab. In der Anfangszeit der PCs wurden an einen durchschnittlichen Computer nur ein Bildschirm und eine Tastatur angeschlossen. Und dementsprechend war der AT aufgebaut: Der einzige spezielle Anschluss auf einem AT-Mainboard war der Tastaturanschluss (Abbildung 6.5).

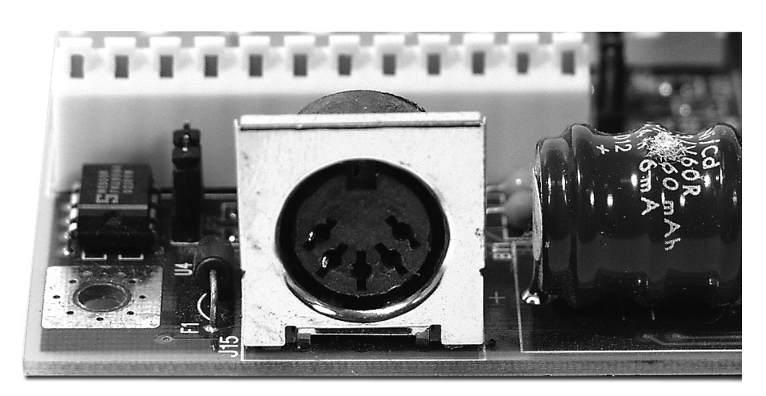


Abb. 6.5: Tastaturanschluss auf der Rückseite eines AT-Mainboards

Mit den Jahren hat die Anzahl der Geräte, die an der Rückseite des PCs angeschlossen werden können, enorm zugenommen. Am durchschnittlichen PC gibt es heute eine Tastatur, eine Maus, einen Drucker, Lautsprecher, einen Bildschirm, und wenn Sie ein System wie ich einsetzen, vier bis sechs USB-Geräte, die jeweils angeschlossen sind. Diese zusätzlichen Komponenten machten einen neuen Formfaktor erforderlich, der mehr Geräteanschlüsse bot. Viele Versuche wurden unternommen, um einen neuen Standard-Formfaktor zu schaffen. Alle diese neuen Formfaktoren hatten zumindest spezielle Anschlüsse für die Maus und den Drucker, und manche hatten sogar Anschlüsse für Bildschirme, Sound und Telefonleitungen.

1001

ATX-Formfaktor

Die andauernde Forderung nach einem neuen Formfaktor mit mehr Standardanschlüssen, der gleichzeitig flexibel genug war, um auch möglichem technologischem Wandel gerecht werden zu können, führte 1995 zur Entwicklung des *ATX-Formfaktors* (Abbildung 6.6). ATX konnte sich anfangs kaum durchsetzen, überflügelte dann aber etwa 1998 AT, wurde zum verbreitetsten Formfaktor und sollte das auch 20 Jahre lang bleiben.

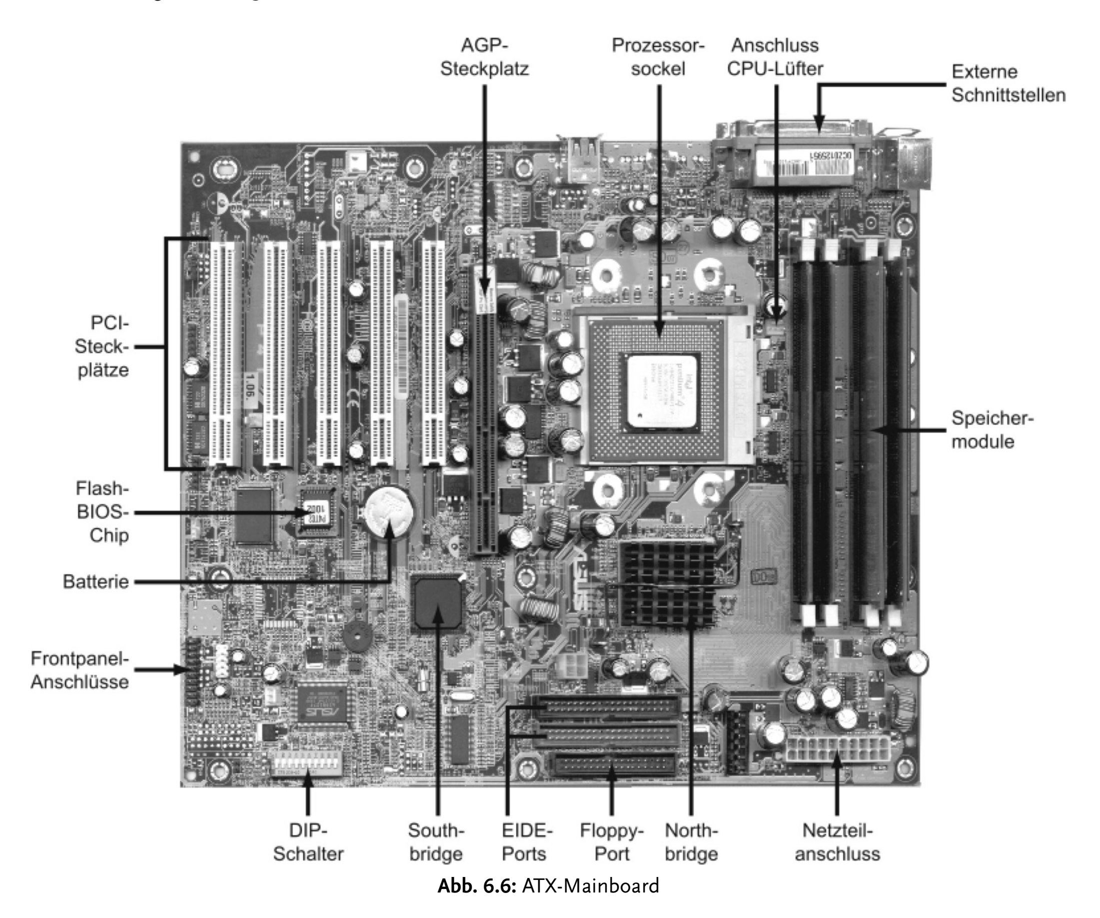


Abb. 6.6: ATX-Mainboard

ATX unterscheidet sich von AT insofern, als es keinen AT-Tastaturanschluss mehr gibt. Dieser wurde durch einen Anschlussbereich ersetzt, der Platz für alle erforderlichen Schnittstellen bietet. Beachten Sie in Abbildung 6.7 auf der linken Seite die Mini-DIN-Anschlüsse (PS/2-Anschlüsse) für Tastatur und Maus, mit denen die allermeisten ATX-Mainboards lange standardmäßig ausgerüstet waren, und an die Sie sich aus Kapitel 2, *Der gläserne PC*, sicher noch erinnern.

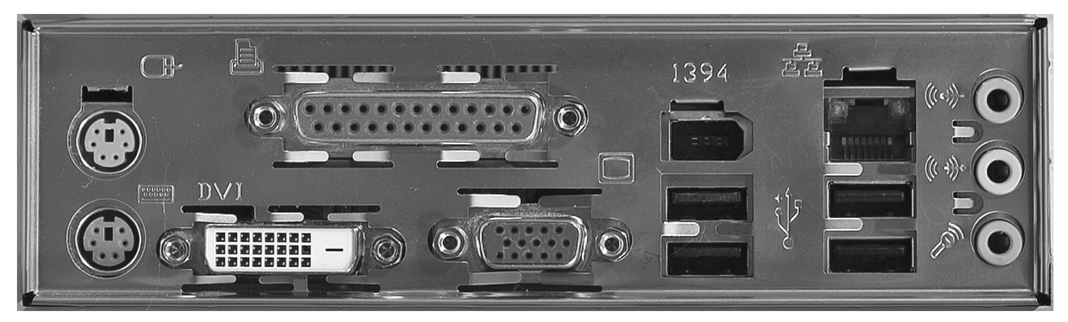


Abb. 6.7: ATX-Anschlussbereich

Der ATX-Formfaktor bietet im Vergleich zum AT-Format zahlreiche Verbesserungen. Beispielsweise sorgt die Platzierung des Netzteils für eine bessere Luftzirkulation im Gehäuseinneren. Die CPU und die Speichermodule sind so angeordnet, dass sie besser zugänglich sind. Die neue Anordnung verhindert, dass langen Erweiterungssteckkarten die CPU oder die Northbridge im Weg sind. Weitere Verbesserungen sorgen ebenfalls für Leistungssteigerungen, wie z.B. die Platzierung des Arbeitsspeichers und der CPU näher an der Northbridge als bei AT-Platinen. Je kürzer die Leitungen, desto leichter lassen sich diese abschirmen, damit sie mit dem doppelten oder vierfachen Mainboard-Takt betrieben werden können. Abbildung 6.8 zeigt ein AT- und ein ATX-Mainboard. Beachten Sie dabei die drastischen Unterschiede bei der Anordnung der internen Anschlüsse.

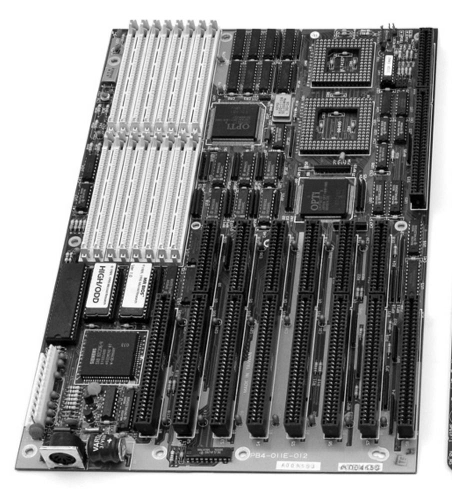
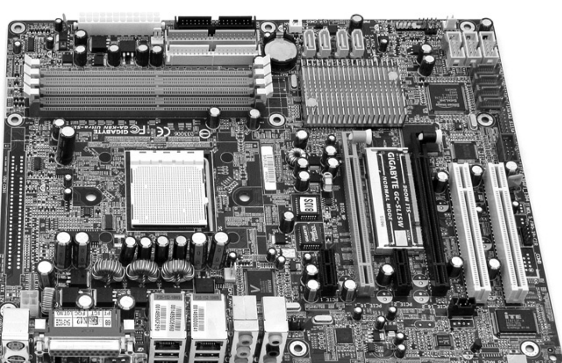



Abb. 6.8: AT- (links) und ATX-Mainboard (rechts) im Vergleich

ATX-Mainboards gibt es in drei Varianten, die den verschiedenen Gehäuseformen angepasst sind. Das ATX-Mainboard mit Abmessungen von ca. 30,5 x 24,5 cm kennen Sie bereits.

Das *microATX*-Mainboard (Abbildung 6.9) ist normalerweise nur etwa 24,5 x 24,5 cm groß und damit etwa 30 Prozent kleiner als ein Standard-ATX-Mainboard, bietet aber weiterhin die Standard-ATX-Anschlüsse. MicroATX-Mainboards lassen sich in herkömmliche ATX-Gehäuse, aber auch in die viel kleineren microATX-Gehäuse einbauen. Allerdings ist zu beachten, dass nicht alle microATX-Gehäuse die exakt gleichen Abmessungen besitzen. microATX wird manchmal auch mit dem griechischen Symbol für Mikro als µATX geschrieben.



Abb. 6.9: Ein microATX-Mainboard

1999 entwickelte Intel eine microATX-Variante, die *FlexATX* genannt wurde. Die minimalen Abmessungen von FlexATX-Mainboards liegen bei nur ca. 23 x 19 cm, sodass es sich hier um die kleinsten Mainboards des ATX-Standards handelt. FlexATX ist heutzutage praktisch vom Markt verschwunden.

ITX-Formfaktor

2001 begann der Chipsatz-Hersteller VIA Technologies damit, ein SFF-Mainboard (*Small Form Factor*) mit der Bezeichnung *ITX* zu entwickeln. ITX war kein sonderlicher Erfolg beschert, aber VIA setzte die Entwicklung fort und stellte sogar noch kleinere Formfaktoren vor, die heutzutage den SSF-Markt bevölkern, insbesondere Mini-ITX.

Mini-ITX ist nur ca. 17 x 17 cm groß und konkurriert mit dem ansonsten nahezu identischen micro-ATX (Abbildung 6.10).



Abb. 6.10: Mini-ITX

Ein großer Vorteil dieser SFF-Mainboards ist der äußerst geringe Energieverbrauch. ITX-Netzteile sind verglichen mit normalen Netzteilen ziemlich klein. Der geringe Energieverbrauch sorgt auch für geringere Wärmeentwicklung und ermöglicht vielen SFF-Systemen eine passive Kühlung ohne Lüfter. Damit sind sie ideal für den Einsatz als Mediacenter-PCs geeignet.

Wichtig

Die CompTIA nennt den ITX-Standard als einen Formfaktor. Reine ITX-Mainboards gibt es zwar nicht, aber Mini-ITX ist ziemlich verbreitet.

Proprietäre Formfaktoren

Einige bedeutende PC-Hersteller fertigen Mainboards, die nur in firmeneigenen Gehäusen eingesetzt werden können. Diese *proprietären* Mainboards ermöglichen den Unternehmen die Fertigung von Systemen, die sich vom sonst Üblichen abheben und keineswegs zufällig dafür sorgen, dass man beim Service und bei Erweiterungen auf autorisierte Händler angewiesen ist. Einige der Merkmale proprie-

tärer Platinen sind Riser-Steckkarten, bei denen Teile der Schaltungen, die sich sonst auf dem Mainboard befinden, auf einer zweiten Platine untergebracht werden, die mit dem Mainboard über ein spezielles Kabel verbunden ist und über proprietäre Anschlüsse für die Stromversorgung verfügt. Früher waren proprietäre Mainboards bei Komplettsystemen verbreitet, aber heutzutage sieht man sie nur selten, wie bei kleinen würfelförmigen Computern.

Tipp: Mainboard-Varianten

Mainboards sind in einer großen Vielfalt von Formfaktoren erhältlich. Besuchen Sie einen Computerhändler und sehen Sie sich das Sortiment an. Achten Sie auch auf die Unterschiede zwischen ATX- micro-ATX- und Mini-ITX-Mainboards.

1. ATX-Mainboards sind gebräuchlich, aber sind auch Mini-ITX-Mainboards oder proprietäre Mainboards verfügbar?
2. Verwenden die Angestellten technischen Jargon und nennen Motherboards »Mobos«? (Dieser Begriff ist im Englischen außerhalb von Lehrbüchern durchaus gebräuchlich.)

6.1.1 Chipsatz

Jedes Mainboard besitzt einen *Chipsatz*, also eigenständige integrierte Schaltkreise, die der CPU als Schnittstelle zu all den anderen Komponenten auf dem Mainboard dienen. Der Chipsatz legt die Eigenschaften des Mainboards auf vielerlei Art und Weise fest. Er bestimmt z.B. den verwendbaren Prozessortyp, Art und Kapazität der Speichermodule und die vom Mainboard unterstützten internen und externen Komponenten. Chipsätze bieten unterschiedliche Funktionen, unterschiedliche Leistung und arbeiten unterschiedlich stabil, wodurch sie erheblich zum Kauf oder zur Empfehlung eines bestimmten Mainboards beitragen können. Gute Techniker kennen die jeweils eingesetzten Chipsätze!

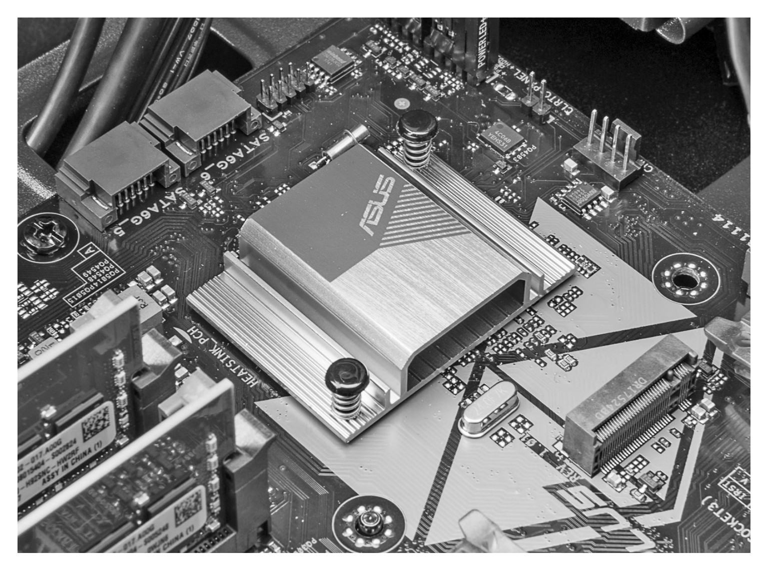


Abb. 6.11: Unter den Kühlkörper verborgener Chipsatz auf einem modernen Mainboard

Da der Chipsatz die Kommunikation zwischen der CPU und anderen Systemkomponenten regelt, befinden sich die Chips, aus denen er besteht, relativ zentral auf dem Mainboard (Abbildung 6.11). Wie Sie aus Kapitel 5 bereits wissen, bestanden Chipsätze ursprünglich aus zwei Chips: Northbridge und Southbridge.

Der Northbridge-Chip unterstützte die CPU bei der Zusammenarbeit mit dem Arbeitsspeicher, während die Southbridge für einige Erweiterungskomponenten und Massenspeichergeräte zuständig war, z.B. für Festplatten. Einige Mainboard-Hersteller fügten einen dritten Chip hinzu (oder tun dies noch immer), der *Super-I/O-Chip* genannt wurde und diese Aufgaben übernahm. Abbildung 6.12 zeigt einen solchen Chip.

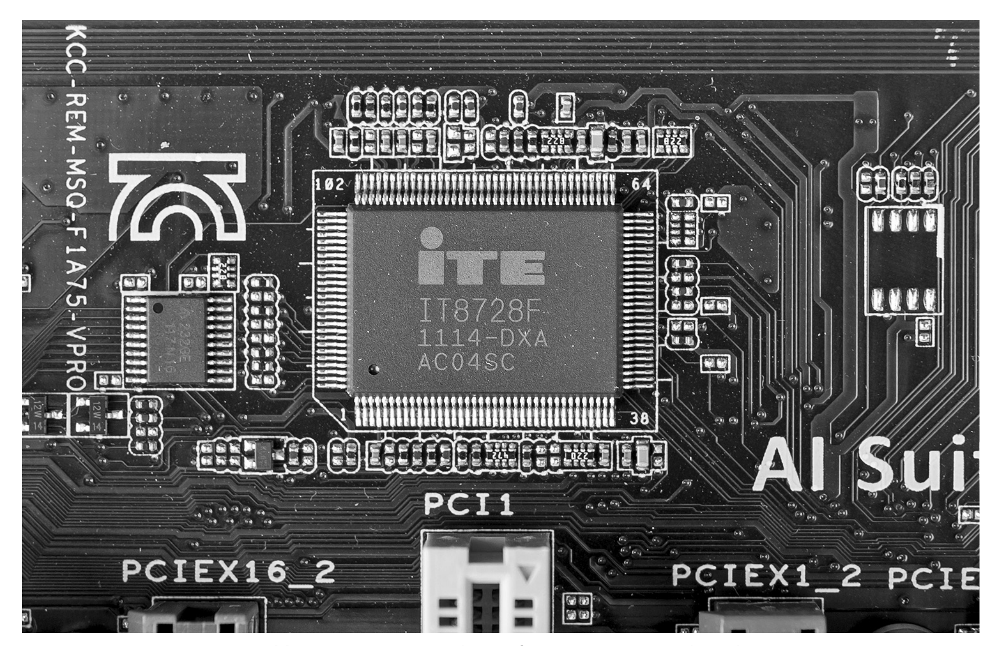


Abb. 6.12: Super-I/O-Chip auf einem ASUS-Mainboard

Inzwischen haben andere Chips viele der Funktionen der klassischen Chipsätze übernommen. Die früher von der Northbridge erledigte Ansteuerung des Arbeitsspeichers übernimmt die CPU selbst. Die Kommunikation mit dem Erweiterungsbus (siehe Abschnitt 6.2, *Erweiterungsbus*), die früher über die Southbridge erfolgte, läuft jetzt auch über die CPU. Die meisten Techniker bezeichnen die verbliebenen Chips auf dem Mainboard als Chipsatz, aber die Begriffe Northbridge und Southbridge sind verschwunden.

Der Chip mit dem System-ROM sorgt für einen Teil des Chipsatz-BIOS, allerdings nur auf grundlegender, allgemeiner Ebene. Der Chipsatz benötigt zusätzliche Unterstützung für seine weiteren Funktionen. Wie kommen aber die Erweiterungskomponenten an ihr BIOS? Dafür sorgen natürlich Softwaretreiber und dasselbe gilt auch für moderne Chipsätze. Sie müssen die passenden Treiber für das jeweils installierte Betriebssystem laden, um alle Funktionen moderner Chipsätze nutzen zu können. Ohne Softwaretreiber können Sie keinen voll funktionsfähigen, stabil arbeitenden PC einrichten. Den meisten Mainboards liegt bei der Auslieferung eine CD oder DVD bei, auf der sich Treiber, Support-Programmen und meist einige zusätzliche Dreingaben befinden, wie z.B. ein Antivirusprogramm (Abbildung 6.13).

Die verschiedenen Chipsätze bieten Unterstützung für eine große Vielfalt unterschiedlicher Hardware, wie etwa Speichersteckplätze (DDR3 oder DDR4), eine gewisse Anzahl von USB-Anschlüssen diverser Versionen, einer Reihe von Massenspeichergeräten, integriertem Netzwerkanschluss, Videoausgabe usw. Abbildung 6.14 zeigt einen Überblick mit typischen Chipsatz-Aufgaben für einen Intel-Z390-Chipsatz.



Abb. 6.13: Treiber-DVD für ein ASUS-Mainboard

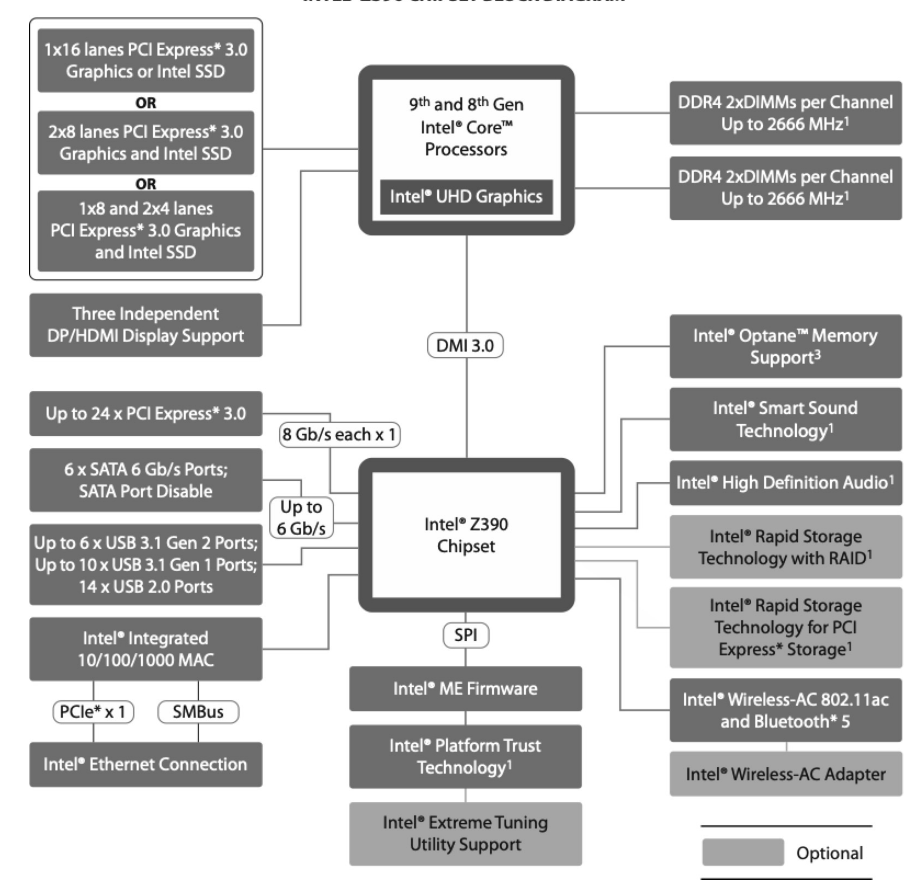


Abb. 6.14: Schaltbild eines modernen Chipsatzes

Gute Techniker sollten die wichtigsten Chipsätze im Detail kennen. Der Chipsatz definiert – bis auf die CPU selbst – fast jede Mainboard-Funktion. Techniker lieben es, über Chipsätze zu sprechen, und erwarten, dass Kollegen die Unterschiede zwischen den verschiedenen Chipsätzen ebenfalls kennen. Außerdem sollten Sie Ihren Kunden Mainboards empfehlen können, die den jeweiligen Anforderungen gerecht werden. In Kapitel 11, *Der maßgeschneiderte PC*, wird die Auswahl von Komponenten beim Zusammenstellen eines PCs für einen bestimmten Zweck, wie z.B. Videoschnitt oder Spiele, eingehend behandelt. Dabei ist die Wahl des richtigen Chipsatzes beim Bau eines solchen Boliden einer der wichtigsten Aspekte.

6.1.2 Standard-Komponenten

Alle Mainboards bieten einen Steckplatz für einen Prozessor (oder zwei) und RAM-Steckplätze. In Kapitel 3 und 4 habe ich eine ganze Reihe davon vorgestellt. Darüber hinaus gibt es Anschlüsse für Massenspeichergeräte wie Festplatten und SSD-Laufwerke (die in Kapitel 8 ausführlich behandelt werden).

6.1.3 Zusätzliche Komponenten

Die Verbindungen und der Funktionsumfang eines Mainboards unterscheiden sich manchmal von denen des Chipsatzes, den das Mainboard verwendet. Diese Diskrepanz entsteht aus mehreren Gründen. Erstens unterstützt ein Chipsatz möglicherweise bis zu acht USB-Anschlüsse, aber um die Kosten niedrig zu halten, baut der Hersteller nur vier Anschlüsse ein. Zweitens können Mainboard-Hersteller zusätzliche Funktionen bereitstellen, die vom Chipsatz nicht unterstützt werden, und zusätzliche Chips einbauen. Ein gängiges Beispiel bilden Mainboards mit Unterstützung für einen seriellen Anschluss. Weitere häufiger anzutreffende, zusätzliche Komponenten sind integrierte Soundchips, Festplatten-RAID-Controller, Netzwerkkarten und anderes. Bei einigen Mainboards gibt es sogar Komponenten, die nur der Bequemlichkeit dienen, wie etwa zusätzliche Stromanschlüsse für Gehäuselüfter oder eine Beleuchtung, damit man sieht, woran man gerade arbeitet.

USB

Alle Chipsätze unterstützen USB, aber nur selten begegnet man zwei Mainboards mit der gleichen Anzahl von Anschlüssen. Mein Mainboard beispielsweise unterstützt acht USB-Anschlüsse, aber auf der Rückseite des Mainboards befinden sich nur vier USB-Anschlüsse (Abbildung 6.15).

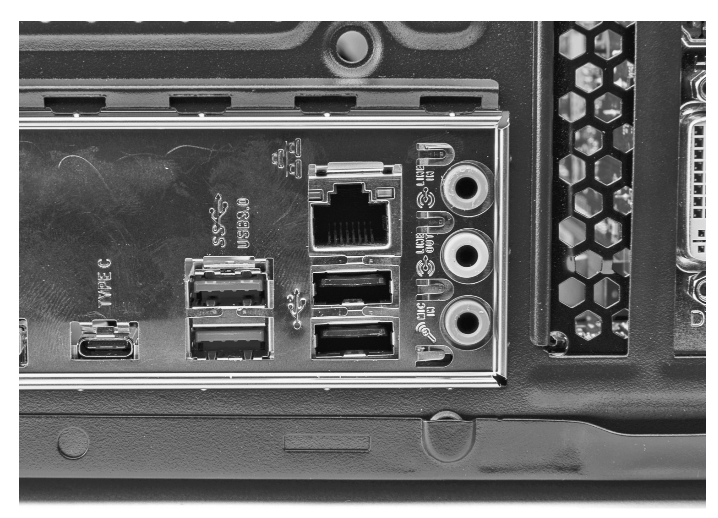


Abb. 6.15: USB-Anschlüsse auf der Rückseite des Rechners

Auf den meisten Mainboards gibt es interne USB-Anschlüsse, die mit einem passenden Kabel an die Vorder- oder Rückseite des Geräts verlegt werden können.

Die Anschlüsse sind standardisiert, deshalb sind viele eingebaute USB-Anschlüsse an der Vorderseite des PC-Gehäuses bereits mit einem entsprechenden Kabel ausgestattet (siehe Abbildung 6.16). Das ist äußerst praktisch, wenn man USB-Geräte verwendet, die häufig ein- und ausgestöpselt werden, wie etwa USB-RAM-Sticks oder Digitalkameras.



Abb. 6.16: USB-Anschlüsse auf der Vorderseite des Rechners

Sound

In den meisten Mainboards sind heute Soundchips integriert. Viele Mainboards besitzen, ähnlich wie für USB, Anschlüsse, um Audiobuchsen an die Vorderseite des Gehäuses zu legen. Sie können Kopfhörer oder Mikrofon dann statt an der Hinterseite an der Vorderseite des PCs anschließen – äußerst praktisch. Diese Anschlüsse sind übrigens mit denen auf Soundkarten identisch. Weitere Informationen finden Sie in Kapitel 10, *Eingabe/Ausgabe*.

Netzwerk

Auf den meisten Desktop-Mainboards gibt es eine RJ-45-Buchse zum Anschließen eines Netzwerkkabels. Die Netzwerkunterstützung ist entweder in den Chipsatz integriert oder wird durch einen zusätzlichen auf dem Mainboard verlöteten Chip bereitgestellt. In Kapitel 18 gehe ich ausführlich auf die physischen Aspekte eines Netzwerks ein.

Video

Viele Mainboards verfügen über eine Videobuchse (oder sogar mehrere) zum Anschließen eines Bildschirms. Diese sind sehr vielfältig und reichen von der älteren VGA-Buchse bis hin zu HDMI-Anschlüssen. In Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*, werden wir ausführlich auf dieses Thema eingehen.

RAID

RAID ist die Abkürzung für *Redundant Array of Independent* (oder auch: *Inexpensive*) *Disks* und bei Mainboards ziemlich häufig anzutreffen. Es gibt viele verschiedene RAID-Typen, aber das RAID auf den Mainboards unterstützt normalerweise nur die *Spiegelung (Mirroring)* oder das *Striping*. Beim Mirroring nehmen zwei Festplatten dieselben Daten auf, was der Datensicherheit dient, da die Daten bei einer defekten Festplatte immer noch unbeschädigt auf der anderen liegen. Beim Striping verhalten sich zwei Festplatten wie ein einziges Laufwerk und die Daten werden abwechselnd auf sie geschrieben, wodurch sich die Geschwindigkeit des Massenspeichers steigern lässt. RAID ist ein sehr interessantes, aber auch komplexes Thema, auf das ich in Kapitel 8, *Festplattentechnologien*, noch näher eingehen werde.

Stromversorgung für Gehäuselüfter

Wie Sie aus Kapitel 3, *Mikroprozessoren*, wissen, besitzen alle Mainboards einen üblicherweise vierpoligen Anschluss, der auch für Lüfter mit dreiadrigen Anschlusskabeln geeignet ist. Einige Mainboards bieten weitere solche Anschlüsse für zusätzliche Gehäuselüfter (deren Kabel tatsächlich meistens dreipolig sind). Im Gegensatz zu Gehäuselüftern, die direkt am Netzteil angeschlossen sind, lassen sich die

am Mainboards angeschlossenen Gehäuselüfter von Windows aus steuern und überwachen – eine nette Zusatzfunktion.

6.2 Erweiterungsbus

Steckplätze für Erweiterungskarten sind seit jeher Bestandteil des PCs. IBM hat den PC damals auch in Hinblick auf zukünftige Entwicklungen entworfen. Der Original-IBM-PC hatte bereits Steckplätze, die in das Mainboard integriert waren, um *Erweiterungskarten* aufzunehmen und damit neue Funktionen für den PC zur Verfügung zu stellen. Die Steckplätze und die damit einhergehenden Leitungen und unterstützenden Chips beim ersten und den modernsten und leistungsfähigsten PCs werden als *Erweiterungsbus* bezeichnet.

6.2.1 Aufbau und Funktion des Erweiterungsbusses

Wie Sie bereits wissen, stehen alle Komponenten im PC, ob nun auf das Mainboard gelötet oder in Sockel eingesetzt, in Verbindung mit dem externen Datenbus und dem Adressbus. Die Steckplätze bilden da keine Ausnahme. Sie sind mit dem übrigen PC über den Chipsatz verbunden. *Wo genau* diese Verbindung hergestellt wird, ist bei den jeweiligen Chipsätzen und Systemen unterschiedlich. Bei neueren Systemen ist der Erweiterungsbus mit der CPU verbunden (Abbildung 6.17), weil moderne CPUs viele Steuerungsaufgaben übernommen haben, die früher zum Chipsatz gehörten. Bei älteren Systemen ist der Erweiterungsbus direkt mit dem Chipsatz verbunden (Abbildung 6.18). Schließlich verfügen viele Systeme über mehrere Arten von Erweiterungsbussen, sodass manche Steckplätze mit der CPU und andere mit dem Chipsatz verbunden sind (Abbildung 6.19).

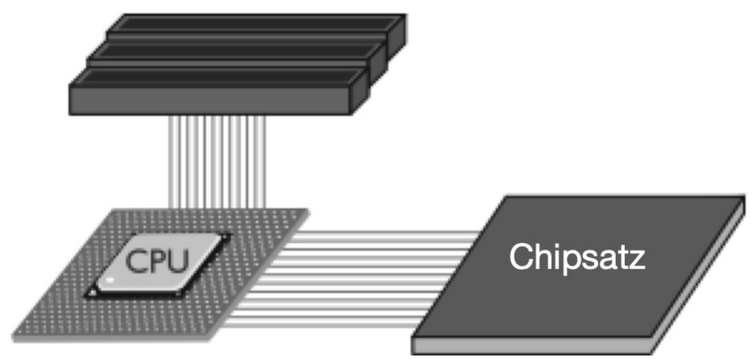


Abb. 6.17: Mit der CPU verbundene Erweiterungssteckplätze

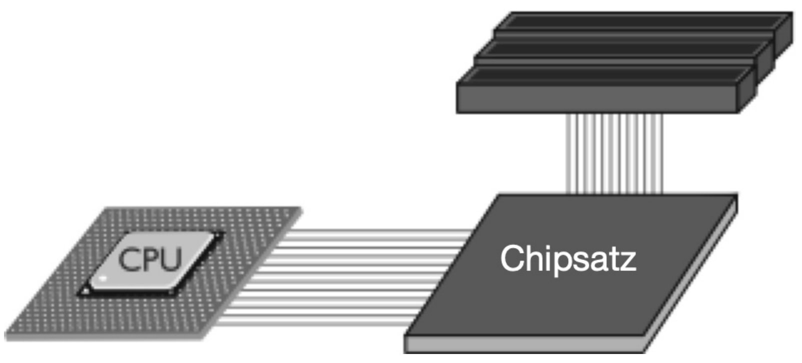


Abb. 6.18: Mit dem Chipsatz verbundene Erweiterungssteckplätze

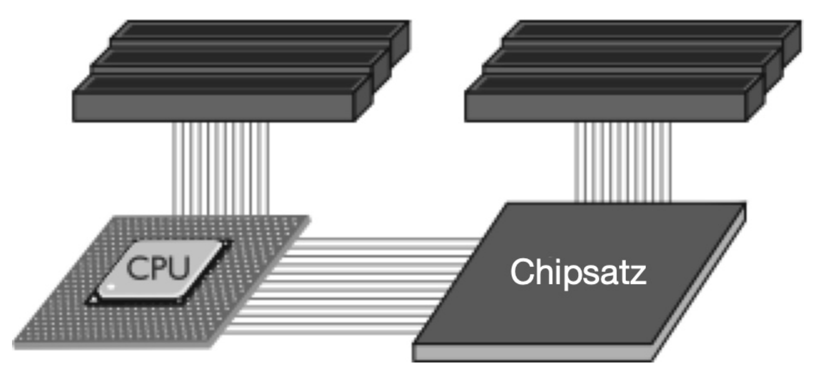


Abb. 6.19: Mit der CPU und dem Chipsatz verbundene Erweiterungssteckplätze

Der Chipsatz sorgt für die Erweiterung des Adress- und Datenbusses bis zu den Erweiterungssteckplätzen und damit zu den Erweiterungskarten in diesen Steckplätzen. Wenn Sie also eine Controller-Karte für Festplatten in einen Erweiterungssteckplatz einsetzen, dann arbeitet diese so, als wäre sie direkt in das Mainboard integriert, wenn auch mit einem großen Unterschied: der Geschwindigkeit. Aus Kapitel 3, *Mikroprozessoren*, wissen Sie, dass der Systemtaktgeber (der Schwingquarz) die CPU antreibt. Der Systemquarz übernimmt eine wichtige Aufgabe im PC und gibt (ähnlich einem Feldwebel, der unablässig »Links! Zwo! Drei! Vier!« brüllt) die Geschwindigkeit für die Aktivitäten im Rechner vor. Alle auf das Mainboard gelöteten Komponenten arbeiten mit der Geschwindigkeit des Systemquarzes. Ein 200-MHz-Mainboard verfügt z.B. zumindest über einen Chipsatz mit Chips, die alle von einem 200-MHz-Quarz angetrieben werden (Abbildung 6.20).

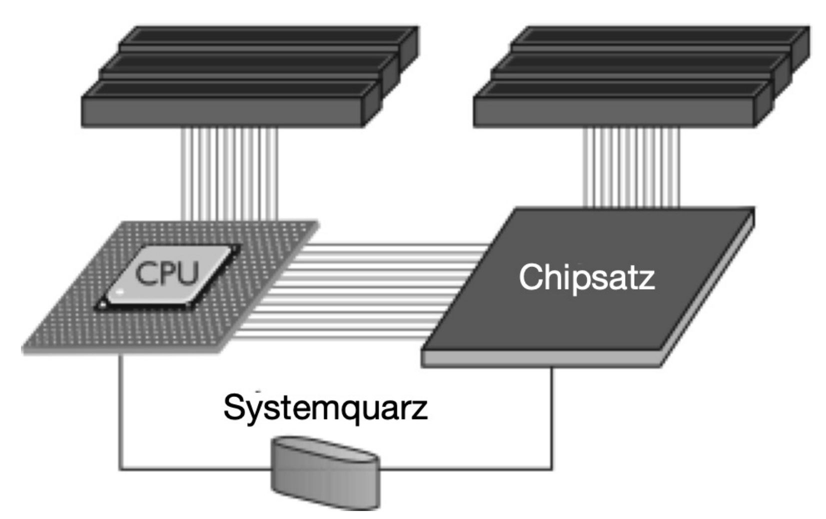


Abb. 6.20: Der Systemtaktgeber gibt die Geschwindigkeit vor.

Quarzoszillatoren treiben nicht nur die CPU und den Chipsatz an. Nahezu alle Chips im Rechner verfügen über eine CLK-Leitung (*Taktleitung*) und müssen vom Taktgeber gesteuert werden, was auch für die Chips auf Erweiterungskarten gilt. Angenommen, Sie kaufen eine Komponente, die nicht zusammen mit dem Rechner geliefert wurde, wie z.B. eine Soundkarte. Die Chips auf der Soundkarte müssen über ein CLK-Signal von einem Taktgeber gesteuert werden. Wenn Sie den Systemquarz für die Steuerung der Soundkarte nutzen würden, müssten die Soundkarten-Hersteller Soundkarten für alle

möglichen Mainboard-Geschwindigkeiten produzieren. Sie müssten eine 100-MHz-Soundkarte für ein 100-MHz-System oder eine 200-MHz-Soundkarte für ein 200-MHz-System kaufen.

Das wäre lächerlich, und das wusste IBM bei der Entwicklung des Personal Computers auch. IBM musste daher dem externen Datenbus eine Erweiterung hinzufügen, die mit einer *eigenen einheitlichen Geschwindigkeit* betrieben werden konnte. Über diesen Teil des externen Datenbusses konnte man dann neue Geräte in den PC integrieren. IBM erreichte dieses Ziel, indem es diesen Teil, der mit den Erweiterungssteckplätzen in Verbindung steht, mit einem anderen Quarzbaustein betrieb (Abbildung 6.21).

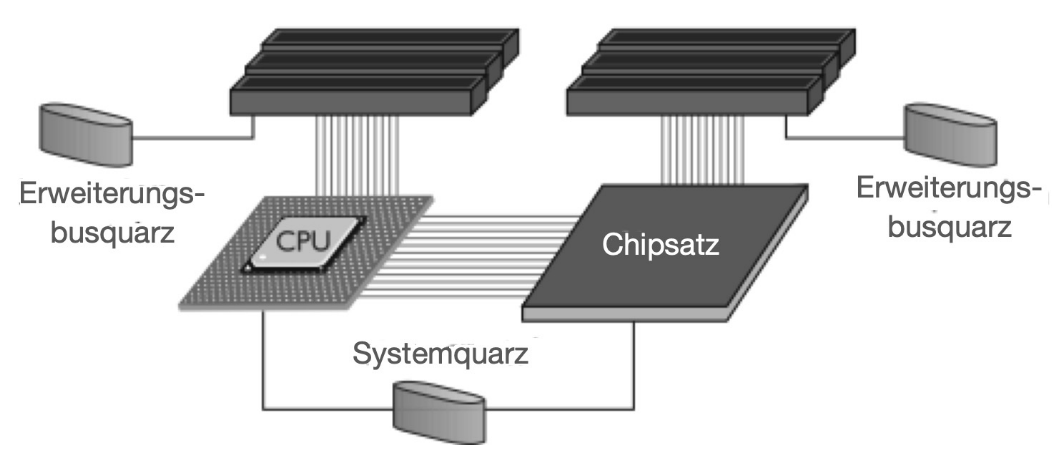


Abb. 6.21: Funktion des System- und des Erweiterungsbusquarzes

Die Erweiterungssteckplätze laufen sehr viel langsamer als der Frontside-Bus. Der Chipsatz verbindet die beiden Busse und gleicht die unterschiedlichen Geschwindigkeiten über Waitstates (Wartezyklen) und spezielle Pufferspeicherbereiche aus. Auf diese Weise können alle Erweiterungssteckplätze unabhängig von der Geschwindigkeit des Mainboards mit einheitlicher Geschwindigkeit betrieben werden. Im Original-IBM-PC betrug diese Geschwindigkeit die Hälfte von 14,318 MHz, also etwa 7,16 MHz. Moderne Erweiterungsbusse laufen sehr viel schneller. Sehen wir uns zunächst PCI an, den ältesten der modernen Erweiterungsbusse.

6.2.2 PCI

Anfang der 1990er führte Intel den PCI-Bus (*Peripheral Component Interconnect*) ein (Abbildung 6.22) und veränderte den PC-Erweiterungsbus damit nachhaltig. Intel traf im Zusammenhang mit PCI viele kluge Entscheidungen, nicht zuletzt die, dass PCI als Public Domain veröffentlicht und damit für andere Hersteller äußerst attraktiv wurde. PCI sorgte für eine breitere, schnellere und flexiblere Alternative zu den bisherigen Erweiterungsbussen. Die außergewöhnliche Technologie des neuen Busses bewirkte in Verbindung mit seiner Lizenzfreiheit schnell, dass die Hersteller sich von den älteren Bussystemen abwandten und PCI übernahmen.

Mit seinen neuen Fähigkeiten mischte PCI die PC-Welt regelrecht auf. Der Original-PCI-Bus war 32 Bit breit und lief mit 33 MHz, was schon ausgezeichnet war, aber diese Funktionen erwartete man und sie waren nicht weltbewegend. PCI war deshalb so interessant, weil er zusätzlich neben anderen Erweiterungsbussen genutzt werden konnte. Als PCI auf den Markt kam, konnte man Mainboards mit PCI- und älteren Steckplätzen kaufen. Das war wichtig, weil die Benutzer auf diese Weise ihre alten Karten weiter verwenden und langsam auf PCI umsteigen konnten. Genauso beeindruckend war, dass PCI-Geräte selbstkonfigurierend waren (und immer noch sind), eine Funktion, die zu dem als *Plug&Play* bezeichneten Industriestandard führte. Und schließlich bot PCI eine leistungsfähige Burst-Mode-Funktion, die sehr effiziente Datenübertragungen ermöglichte.

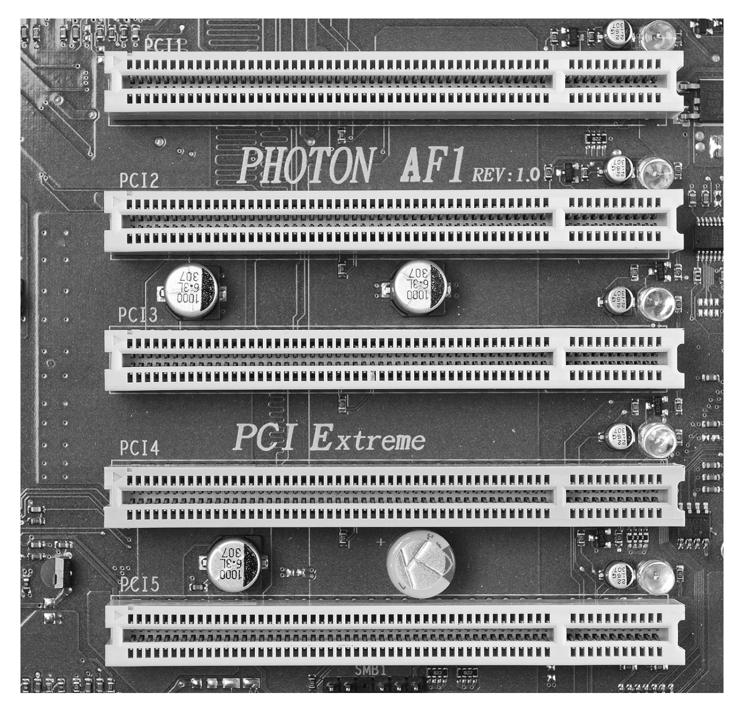


Abb. 6.22: PCI-Erweiterungsbus-Steckplätze

6.2.3 Mini-PCI

Dank des speziellen *Mini-PCI*-Formats schaffte PCI es sogar in die Laptops (Abbildung 6.23). Mini-PCI benötigt wenig Strom und die Karten liegen flach, was bei Laptop-Steckplätzen wichtig ist! Mini-PCI finden Sie allerdings ebenso wie normale PCI-Steckplätze nur noch in älteren Computern.

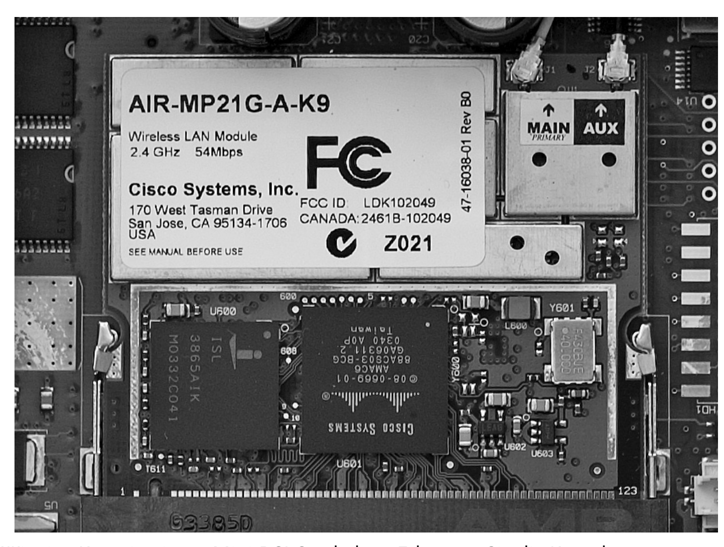


Abb. 6.23: Winzige Karte in einem Mini-PCI-Steckplatz. Erkennen Sie die Kontakte am unteren Bildrand?

6.2.4 PCI Express

PCI Express (*PCIe*) ist zwar immer noch PCI, ersetzt die gemeinsam genutzten parallelen Kommunikationsverbindungen über den Bus aber durch serielle Punkt-zu-Punkt-Verbindungen. Betrachten Sie einen einzigen 32-Bit-Datenblock, der von einer Komponente zur CPU übertragen werden soll. Bei der parallelen Kommunikation übertragen 32 Leitungen jeweils ein Bit dieser Daten, bei der seriellen Kommunikation hingegen überträgt nur eine Leitung diese 32 Bit. Sie denken vielleicht, 32 Leitungen sind besser als eine, richtig?

Nun, erstens nutzt PCIe den Bus nicht gemeinsam. Jedes PCIe-Gerät hat seine eigene Direktverbindung (eine Punkt-zu-Punkt-Verbindung) zur CPU, muss also nicht auf andere Geräte warten. Bei wirklich schnellen Datentransfers (ab etwa einem Gigabit pro Sekunde) wird es zweitens schwierig, alle 32 Datenbits wirklich gleichzeitig zur anderen Komponente zu befördern, weil einige Bits dort möglicherweise (aufgrund geringfügig unterschiedlicher *Signallaufzeiten*) ein wenig früher als andere ankommen. Dadurch müssten die ankommenden Daten aber in Höchstgeschwindigkeit daraufhin überprüft werden, ob auch alle Bits im richtigen Format eingetroffen sind. Bei seriellen Daten kann dieses Problem nicht auftreten, weil die Bits in einem einzigen Datenstrom nacheinander eintreffen. Bei wirklich schnellen Datentransfers sind einzelne Punkt-zu-Punkt-Verbindungen tatsächlich schneller als Parallelverbindung mit mehreren Leitungen.

Und PCIe ist wirklich verdammt schnell! PCIe-Verbindungen verwenden eine Leitung zum Senden und eine für den Empfang. Diese Leitungspaare zwischen PCIe-Controller und den einzelnen Komponenten werden *Lanes* genannt. Die Lanes arbeiten bei PCIe 1.x mit 2,5 Gigatransfers pro Sekunde (GTps) bzw. bei PCIe 2.x mit 5,0 GTps, bei PCIe 3.x mit 8 GTps und bei PCIe 4.0 mit satten 16 GTPs! Es kommt noch besser: Jede Punkt-zu-Punkt-Verbindung kann 1, 2, 4, 8, 12 oder 16 Lanes nutzen und so theoretisch eine maximale Bandbreite von 256 GTps erreichen. Die Transferrate gibt die Anzahl der Operationen pro Sekunde an. Die effektive Rate verringert sich aufgrund des *Codierungsverfahrens* (die Art, wie die Daten aufgeteilt und wieder zusammengefügt werden) zwar noch ein wenig, aber die Datenrate kann im Vollduplex-Betrieb maximal beeindruckende 32 GBps bei einer x16-Verbindung erreichen.

Wichtig

Für die CompTIA A+-Prüfung 220-1001 müssen Sie die verschiedenen Erweiterungssteckplätze kennen, insbesondere PCI und PCIe.

Bei den verbreitetsten PCIe-Steckplätzen handelt es sich um die Variante mit 16 Lanes (x16), die zumeist für Grafikkarten verwendet wird (Abbildung 6.24). Auf den ersten PCIe-Mainboards befanden sich zumeist ein einzelner PCIe-x16-Steckplatz und mehrere der üblichen PCI-Steckplätze. (Erinnern Sie sich noch daran, dass PCI mit anderen Steckplätzen und damit auch mit anderen PCI-Varianten kombiniert werden kann?) Übrigens gibt es PCIe-Steckplätze auch in einer Variante mit kleinem Formfaktor für Mobilrechner, der *PCI Express Mini* Card heißt und in Kapitel 23, *Tragbare Computer*, ausführlich zur Sprache kommt.

Die Bandbreite eines x16-Steckplatzes ist so hoch, dass bestenfalls Grafikkarten diese nutzen können. Daher besitzen die meisten PCIe-Mainboards auch Steckplätze mit weniger Lanes. Momentan ist x1 (Abbildung 6.25) die gebräuchlichste PCIe-Steckplatzvariante, x4-Steckplätze sind aber auch gebräuchlich.

Tipp: Einkaufstour

Wie sieht das neueste PCIe-Mainboard aus? Suchen Sie online oder beim örtlichen Computerhändler nach hochwertigeren Mainboards. Welche Kombinationen von PCIe-Varianten sind auf einem einzigen Mainboard verfügbar? Notieren Sie die Ergebnisse und vergleichen Sie sie mit denjenigen Ihrer Kollegen.



Abb. 6.24: PCIe-x16-Steckplatz (Mitte) und PCI-Steckplätze (oben/unten)

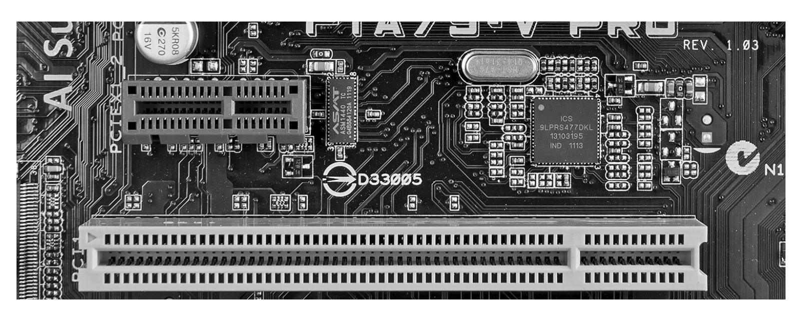


Abb. 6.25: PCIe-x1-Steckplatz (oben)

6.2.5 Erweiterungskarten installieren

Die erfolgreiche Installation von Erweiterungskarten zählt zu den alltäglichen Aufgaben von Technikern, die in mindestens vier Schritten erfolgt. Zunächst einmal müssen Sie wissen, ob die Karte vom System und dem verwendeten Betriebssystem unterstützt wird. Dann müssen Sie die Karte ordnungsgemäß in einen Erweiterungssteckplatz einsetzen, ohne die Karte selbst oder das Mainboard dabei zu beschädigen. Danach müssen Sie die *richtigen* Treiber für das *jeweilige* Betriebssystem installieren. Im vierten und letzten Schritt schließlich sollten Sie dann stets prüfen, ob die Karte auch wirklich korrekt funktioniert, bevor Sie Ihre Arbeit als erledigt betrachten.

Wichtig

Die vier Schritte zur Installation einer Erweiterungskarte gelten für sämtliche Typen. In der CompTia A+-Prüfung kommen sowohl die üblicherweise verwendeten wie Sound-, Grafik- und Netzwerkkarten vor, aber auch bestimmte Erweiterungskarten für USB- oder Thunderbolt-Verbindungen. Außerdem wird nach folgenden Kartentypen gefragt: Karten für drahtlose Netzwerke und Mobilfunknetzwerke, Speicherkarten, TV-Empfängerkarten, Videoaufzeichnungskarten, Riser-Karten und weitere, die ich in den jeweiligen Kapiteln des Buchs ausführlich erörtere. Bei der Installation folgen Sie stets den vier Schritten: Wissen, Einbau, Gerätetreiber und Überprüfung.

Schritt 1: Wissen

Versuchen Sie bereits vor dem Kauf, möglichst viel über die einzubauende Komponente zu erfahren! Funktioniert sie im jeweiligen Rechner unter dem eingesetzten Betriebssystem? Gibt es Treiber für dieses Betriebssystem? Wenn Sie ein neueres Windows benutzen, dann lautet die Antwort auf diese Fra-

gen fast immer »Ja«. Wenn Sie aber ein älteres oder ein weniger gebräuchliches Betriebssystem wie Linux einsetzen, dann werden diese Fragen kritisch. Ein Großteil der älteren Hardwarekomponenten funktioniert unter neueren Windows-Versionen schlichtweg gar nicht, insbesondere dann, wenn Sie Windows 10 nutzen. Lesen Sie die Dokumentation und überzeugen Sie sich auf der Website der Hersteller davon, dass Sie auch die richtigen Treiber haben. Prüfen Sie dabei auch, ob Ihnen die neuesten Treiber vorliegen, denn für viele Geräte gibt es ziemlich häufig neue Treiberversionen.

Schritt 2: Einbau

Um eine Erweiterungskarte erfolgreich zu installieren, müssen Sie Maßnahmen ergreifen, die eine Beschädigung der Karte und des Mainboards ausschließen. Sie müssen also wissen, wie Sie mit Steckkarten umgehen, wie *elektrostatische Entladungen* (*ESD*) vermieden werden können, und ganz allgemein mit Elektronik vertraut sein. Zudem müssen Sie die Steckkarte korrekt und sicher in einen verfügbaren Erweiterungssteckplatz einsetzen.

Im Idealfall befindet sich die Karte an einem von zwei Orten: im Computer oder in einer antistatischen Verpackung. Beim Einsetzen oder Ausbauen einer Karte sollten Sie diese vorsichtig an den Rändern anfassen. Berühren Sie nicht die Kontaktleisten und auch nicht die Bauteile auf der Platine (Abbildung 6.26).

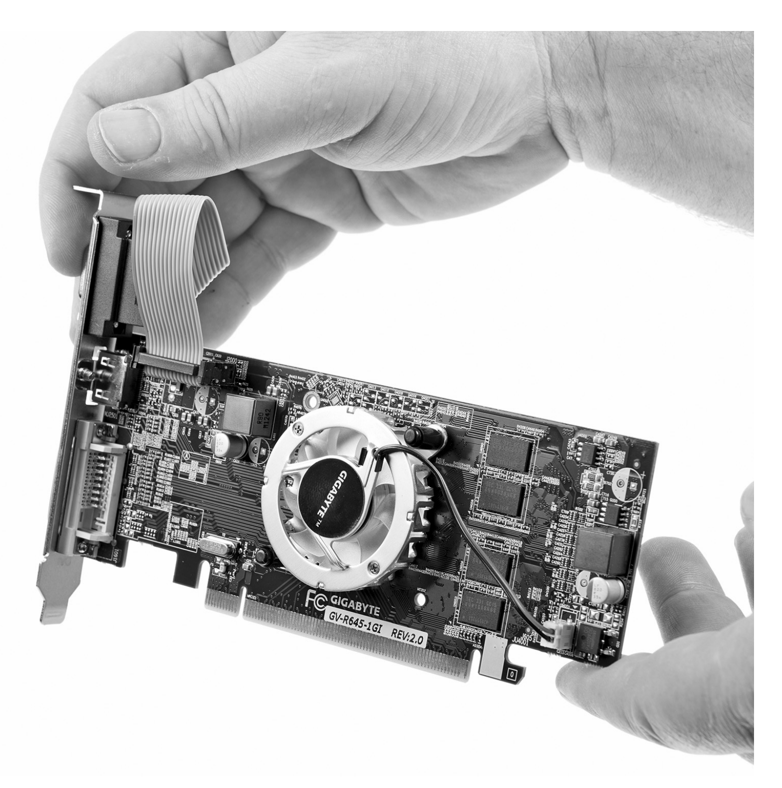


Abb. 6.26: An diesen Stellen dürfen Sie die Steckkarte berühren.

Verwenden Sie möglichst ein Antistatikarmband und verbinden Sie es, wie in Kapitel 1, *Sicherheit und Professionalität*, beschrieben, mit dem PC. Wenn Sie kein Antistatikarmband besitzen, dann können Sie das Verfahren benutzen, das Techniker häufig nutzen, um ESD zu vermeiden, und das Netzteil bzw. eine blanke (nicht lackierte) Stelle des Rechnergehäuses berühren, nachdem Sie die Erweiterungskarte aus ihrer antistatischen Verpackung entfernt haben. Damit sorgen Sie dafür, dass Sie, die

Karte und der PC dasselbe elektrische Potenzial besitzen, und minimieren so die Gefahr elektrostatischer Entladungen.

Bei modernen Systemen fließt immer ein wenig Strom auf dem Mainboard, sofern der Rechner an das Stromnetz angeschlossen ist. In Kapitel 7, *Netzteile*, werden die Stromversorgung und der Umgang mit Elektrizität ausführlich behandelt, weshalb hier eine Kurzversion genügen soll: *Trennen Sie den Rechner immer von der Stromversorgung, bevor Sie Erweiterungskarten einsetzen!* Wenn Sie dies versäumen, können die Karte und/oder das Mainboard beschädigt werden. Und das ist das Risiko nicht wert!

Achten Sie beim Einsetzen oder Entfernen einer Karte darauf, dass diese sich nicht verkantet. Steckkarten können dadurch beschädigt werden. Ein kleiner Winkel ist dagegen in Ordnung und zum Ausbau der Karte oft sogar erforderlich. Schrauben Sie die Karte immer gut im Gehäuse fest, damit sie sich nicht lockern und eventuell Kurzschlüsse mit anderen Karten verursachen kann. Viele Karten werden über ihre Schraubverbindungen zudem zusätzlich über das Gehäuse geerdet (Abbildung 6.27).



Abb. 6.27: Schrauben Sie Steckkarten immer gut fest.

Viele Techniker meinen, dass man die Kontaktleisten von Karten, die nicht richtig funktionieren, reinigen sollte. Das ist nach der Installation der Karte jedoch meist nicht erforderlich und kann bei unsachgemäßer Ausführung sogar zu Beschädigungen führen. Eine Reinigung sollten Sie nur dann durchführen, wenn die Karte längere Zeit gelagert wurde und die Kontakte offensichtlich verschmutzt sind.

Verwenden Sie dazu niemals einen Radiergummi, denn dabei können Rückstände zwischen Steckkontakt und Sockel geraten, die den Kontakt verhindern und für den Ausfall der Karte sorgen können. Benutzen Sie einen Kontaktreiniger, der genau für diesen Zweck gedacht ist und die Kontakte zuverlässig reinigt, aber keine Rückstände hinterlässt. Derartige Reiniger sind bei jedem Elektronikfachhändler oder natürlich online erhältlich.

Wenn das Mainboard korrekt eingebaut wurde, dann schließt eine vollständig eingesetzte Erweiterungskarte plan mit der Rückseite des PC-Gehäuses ab, ohne dass zwischen dem Slotblech der Karte und dem Schraubloch am Gehäuse eine Lücke bleibt. Wenn die Karte richtig sitzt, dann sollten die Kontaktleisten im Steckplatz nicht mehr sichtbar sein. Abbildung 6.28 zeigt eine korrekt sitzende Erweiterungskarte, die sauber im Steckplatz sitzt.

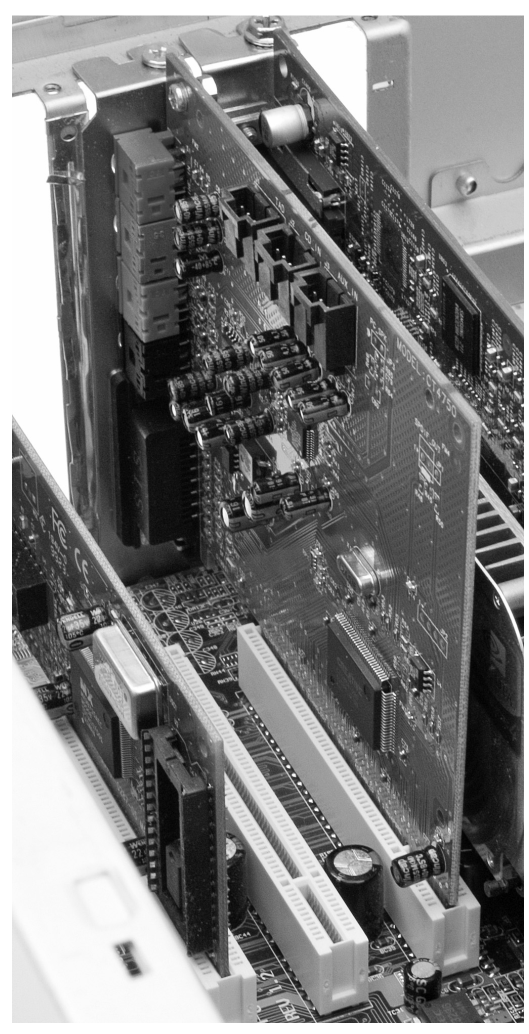


Abb. 6.28: Korrekt sitzende Erweiterungskarte. Beachten Sie den geraden Sitz der Steckkarte und wie dicht das Slotblech mit dem Gehäuse abschließt.

Schritt 3: Gerätetreiber

Wie Sie aus Kapitel 5, *BIOS und CMOS*, wissen, benötigen alle Komponenten, unabhängig davon, ob sie in das Mainboard integriert sind oder anderweitig hinzugefügt wurden, ein BIOS. Bei fast allen Erweiterungskarten wird dieses BIOS in Form von Gerätetreibern zur Verfügung gestellt, die vom Betriebssystem automatisch geladen oder von einer vom Hersteller mitgelieferten CD oder DVD auf den Rechner übertragen werden.

Die Installation von Gerätetreibern ist eigentlich ganz einfach. Natürlich sollten Sie die zur Komponente und zum Betriebssystem passenden Treiber installieren. Das liegt zwar auf der Hand, aber wundern Sie sich nicht, wenn hier Fehler gemacht werden. Bei der Aktualisierung von Treibern müssen Sie zudem möglicherweise erst die alten Treiber deinstallieren, bevor Sie die neuen installieren können. Und wenn Probleme auftreten, dann müssen Sie schließlich die gerade erst geladenen Treiber wieder deinstallieren oder die zuletzt installierten (und hoffentlich stabileren) Treiber wiederherstellen.

Beschaffung der richtigen Treiber Um sicherzustellen, dass der bestmögliche Treiber für die Komponente verwendet wird, sollten Sie immer die Website des Herstellers bzw. Anbieters aufsuchen. Die mit der Komponente gelieferten Treiber mögen zwar funktionieren, aber es ist einigermaßen wahrscheinlich, dass es neuere und/oder bessere Treiber auf der Website gibt. Wie können Sie aber wissen, ob die Treiber auf der Website neuer sind? Werfen Sie dazu einfach zunächst einen Blick auf die Treiber-CD, da dort manchmal die Version aufgedruckt ist. Wenn das nicht der Fall ist, dann müssen Sie die CD in ein Laufwerk einlegen und sich darauf ein wenig umsehen. Oft zeigt das bei aktivierter Autoplay-Funktion automatisch gestartete Programm die Versionsnummer an. Wenn beides nicht der Fall ist, dann sollten Sie auf dem Datenträger nach Readme-Dateien suchen (Abbildung 6.29).

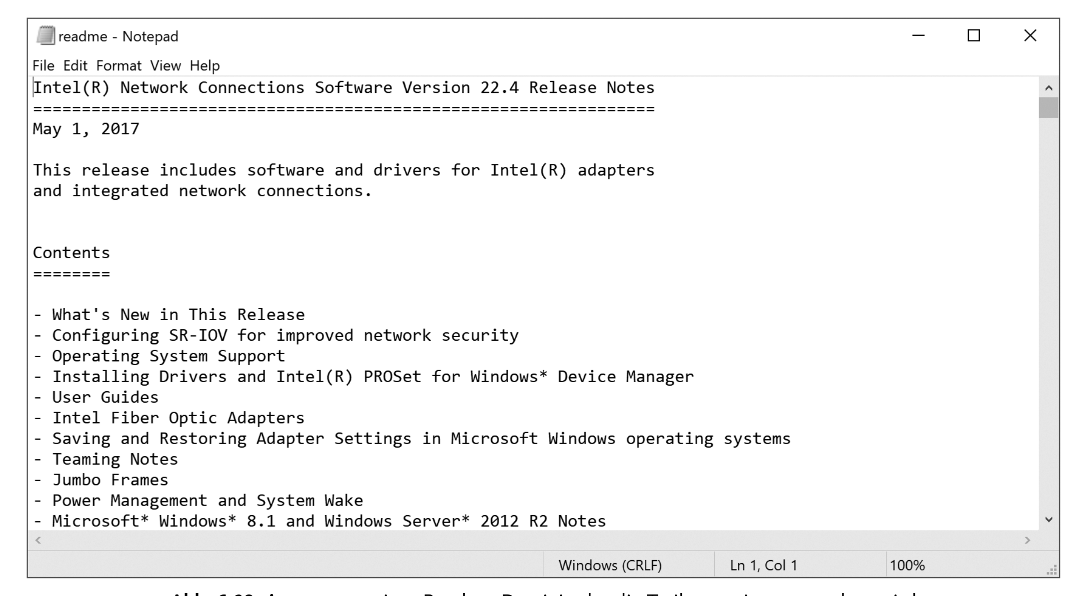


Abb. 6.29: Auszug aus einer Readme-Datei, in der die Treiberversion angegeben wird

Treiber oder Gerät zuerst installieren? In fast allen Fällen sollten Sie den Gerätetreiber nach dem Gerät installieren. Wenn das Gerät noch nicht installiert ist, kann es bei der Treiberinstallation auch nicht erkannt werden und es kommt zu Fehlern. Die Ausnahmen von dieser Regel sind USB-Geräte – hier müssen für gewöhnlich erst die Treiber installiert werden! (Im Fall von Thunderbolt, einer weiteren exzellenten externen Anschlussmöglichkeit, spielt die Reihenfolge auf macOS keine Rolle. Und unter Windows? Da hängt es komplett vom Hersteller der Hardware ab. Lesen Sie die Dokumentation.)

Entfernen alter Treiber Bei einigen Karten, wie z.B. Grafikkarten unterschiedlicher Hersteller, müssen erst die alten Treiber entfernt werden, bevor die neue Komponente installiert werden kann. Dazu müssen Sie erst den Treiber im Geräte-Manager ausfindig machen. Klicken Sie mit der rechten Maustaste auf den Gerätetreiber, der entfernt werden soll, und wählen Sie im Kontextmenü DEINSTALLIEREN (Abbildung 6.30).

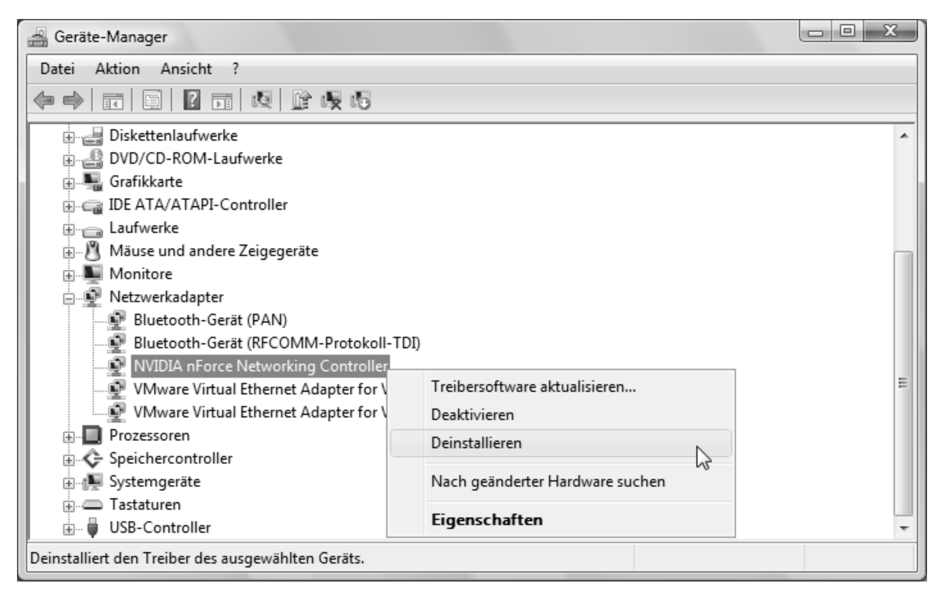


Abb. 6.30: Deinstallieren eines Geräts

Unsignierte Treiber Microsoft will wirklich, dass Ihr Rechner tadellos funktioniert und bietet für Hardwarehersteller ein ausgezeichnetes und strenges Testprogramm an, das *Windows Hardware Certification Program* Zur Bestätigung, dass sie von Microsoft geprüft und für gut befunden wurden, werden die Treiber digital signiert.

Die letzten 32-Bit-Versionen von Windows unterstützten unsignierten Treiber, also Treiber, die das *Windows Certification Program* (wie es damals noch hieß) nicht absolviert hatten. Solche Treiber wurden von Microsoft nicht signiert. Wenn Windows einen solchen Treiber erkennt, zeigt es einen Furcht einflößenden Warnbildschirm an (Abbildung 6.31), der auf die Installation eines nicht signierten Treibers aufmerksam macht. In der CompTIA A+-Prüfung 1001 können unsignierte Treiber vorkommen, auf modernen Windows-Rechnern sind sie jedoch nicht mehr zu finden.



Abb. 6.31: Hinweis auf einen nicht signierten Treiber

Installation neuer Treiber Es gibt zwei Möglichkeiten, neue Treiber zu installieren: Lassen Sie Windows die neue Hardware erkennen und den richtigen Gerätetreiber finden. Die zweite Möglichkeit ist die manuelle Installation durch Verwendung der Installations-CD oder das Herunterladen aus dem Internet. Die meisten Installations-Programme bieten Menüs, über die Sie detailliert festlegen können, was installiert werden soll (Abbildung 6.32).

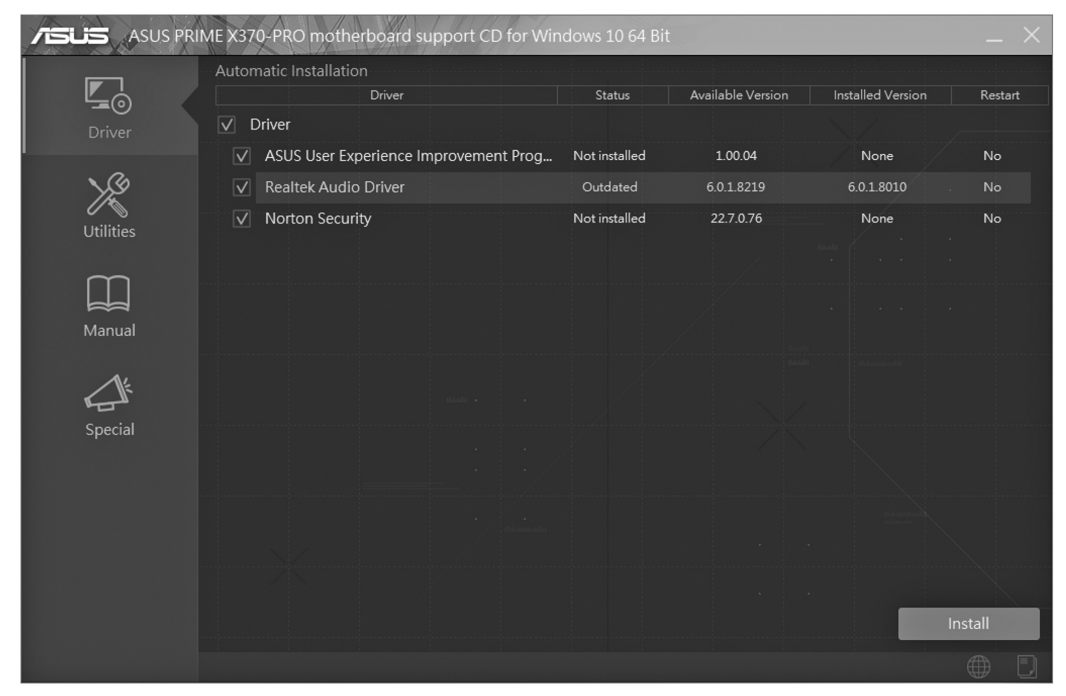


Abb. 6.32: Installationsmenü

Vorherigen Treiber verwenden (Driver Rollback) Alle Windows-Versionen enthalten eine Funktion, die englisch *Driver Rollback* genannt wird und mit der Sie nach der Installation oder Aktualisierung eines Treibers wieder zur zuletzt verwendeten Version zurückkehren können. Wenn Sie gerne mit dem Feuer spielen und z.B. Beta-Treiber für eine Grafikkarte installieren und das System anschließend fürchterlich instabil wird, dann können Sie wieder zu den Treibern zurückkehren, die zuvor funktioniert haben. (Natürlich habe ich diese Funktion nie in Anspruch nehmen müssen!) Um auf diese Funktion zuzugreifen, starten Sie einfach den Geräte-Manager und lassen sich die Eigenschaften der betreffenden Komponente anzeigen. Abbildung 6.33 zeigt die Registerkarte TREIBER und die für die beschriebene Funktion zuständige Schaltfläche VORHERIGER TREIBER.

Hinweis

Um Treiber auf einem Windows-Rechner installieren zu können, benötigen Sie die entsprechenden *Rechte*. Dabei geht es nicht darum, dass Sie jemanden fragen müssten, ob Sie Geräte und Treiber installieren dürfen. Rechte werden unter Windows vergeben, um Benutzern bestimmte Aktionen zu erlauben, wie z.B. das Hinzufügen von Druckern oder das Installieren von Programmen, oder sie eben davon abhalten zu können. Um Treiber installieren zu können, benötigen Sie *administrative Rechte*. Siehe dazu Kapitel 13, *Benutzer, Gruppen und Berechtigungen*.



Abb. 6.33: Zuvor installierten Treiber wieder für eine Komponente verwenden

Schritt 4: Überprüfung

Im letzten Schritt werden das Ergebnis der Installation und die fehlerfreie Funktion der Komponente überprüft. Unmittelbar nach der Installation sollten Sie den Geräte-Manager starten und prüfen, ob Windows die Komponente erkannt hat (Abbildung 6.34).

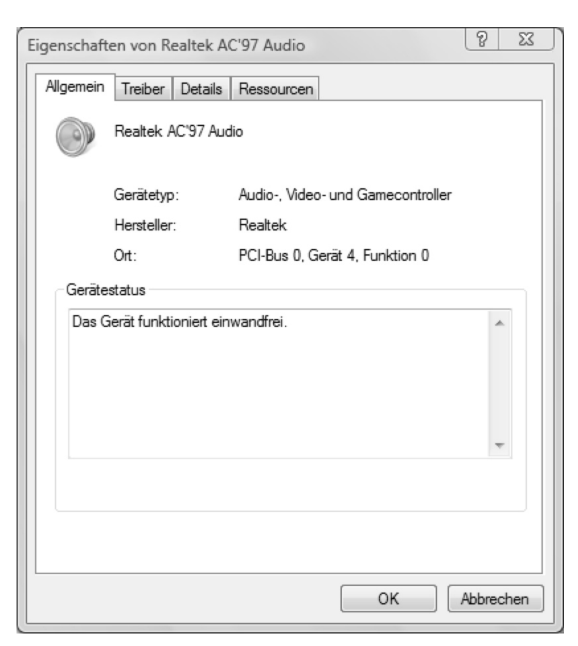


Abb. 6.34: Der Geräte-Manager zeigt an, dass das Gerät ordnungsgemäß funktioniert.

Wenn der Geräte-Manager anzeigt, dass die Komponente fehlerfrei funktioniert, probieren Sie das Gerät aus und prüfen Sie, ob es seine Aufgabe auch wirklich erfüllt. Wurde ein Drucker oder ein Scanner installiert, dann drucken Sie z.B. etwas aus oder scannen etwas ein. Wenn das funktioniert, dann sind Sie fertig!

Vorsicht

Viele PC-Freaks versuchen, auch noch das letzte Quäntchen Leistung aus dem Rechner herauszuholen, ähnlich wie Auto-Enthusiasten, die Motoren tunen, um ein paar PS mehr aus ihnen herauszukitzeln. Die Hersteller von Erweiterungskarten mögen diese Enthusiasten, die noch nicht ganz fertige Treiber (*Beta-Treiber*) kostenlos testen. Beta-Treiber arbeiten meist durchaus zuverlässig, können aber hier und da auch für überraschende Systeminstabilitäten sorgen, was nie gut sein kann! Wenn Sie Beta-Treiber einsetzen, sollten Sie auch wissen, wie Sie diese deinstallieren oder wieder zur vorherigen Version zurückkehren können.

6.2.6 Fehlersuche bei Erweiterungskarten

Korrekt installierte Erweiterungskarten bereiten – im Gegensatz zur Installation selbst – selten Probleme. Sehr wahrscheinlich müssen Sie sich bei der Installation von Erweiterungskarten irgendwann auf Fehlersuche begeben, meist dann, wenn Sie es selbst vermasselt haben.

Die ersten Anzeichen einer fehlerhaft installierten Karte zeigen sich normalerweise sofort, wenn sie ihre Aufgaben erfüllen soll, aber nicht funktioniert. Dann sollten Sie, nach erfolgter Prüfung im Geräte-Manager, erst einmal versuchen, die Komponente erneut zu installieren.

Andere Kapitel in diesem Buch befassen sich mit der Fehlersuche bei speziellen Hardwarekomponenten, wie z.B. bei Grafikkarten (Kapitel 17) und Soundkarten (Kapitel 10). Nutzen Sie diesen Abschnitt als allgemeine Anleitung, um besser entscheiden zu können, worauf Sie achten und wie Sie mit Problemen umgehen sollten.

Der Geräte-Manager ist unter Windows die erste Anlaufstelle bei der Diagnose und Problembehebung. Wenn nach der Installation einer neuen Komponente etwas nicht funktioniert, können Sie im Geräte-Manager viele nützliche Hinweise finden.

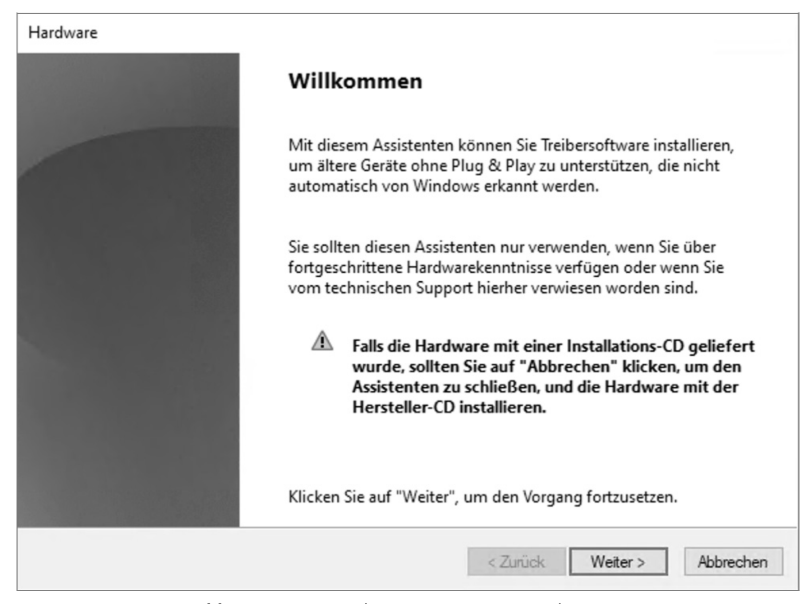


Abb. 6.35: Der Hardware-Asistent in Windows 10

Gelegentlich werden neue Komponenten im Geräte-Manager noch nicht einmal angezeigt. Dann prüfen Sie, ob die Komponente physisch korrekt installiert wurde und mit Strom versorgt wird. Starten Sie dann den Hardware-Assistenten und sehen Sie nach, ob Windows das Gerät nun erkennt. Den Hardware-Assistenten starten Sie durch Klick auf START und Eingabe von `hdwwiz.exe` in das Suchfeld (Abbildung 6.35).

Wenn das Gerät im Geräte-Manager immer noch nicht angezeigt wird, liegt eines von zwei Problemen vor: Entweder ist das Gerät physisch defekt und muss ersetzt werden oder es handelt sich nicht um eine Erweiterungskarte, sondern um eine integrierte Komponente, die im CMOS-Setup deaktiviert wurde.

Nur selten werden Komponenten vom Geräte-Manager gar nicht erkannt. Viel häufiger werden diese erkannt und Hinweise auf bestehende Probleme im Geräte-Manager als Fehlersymbole angezeigt:

- Ein schwarzes »!« in einem Dreieck weist auf eine Komponente hin, die fehlt bzw. von Windows nicht erkannt wurde, oder darauf, dass Treiberprobleme vorliegen (Abbildung 6.36). Manchmal funktionieren Komponenten selbst dann, wenn dieser Fehler gemeldet wird.
- Ein schwarzer, nach unten zeigender Pfeil auf weißem Grund weist auf eine deaktivierte Komponente hin. Meist handelt es sich dabei um manuell deaktivierte oder defekte Geräte. Geräte mit solch einem Fehler funktionieren nicht.

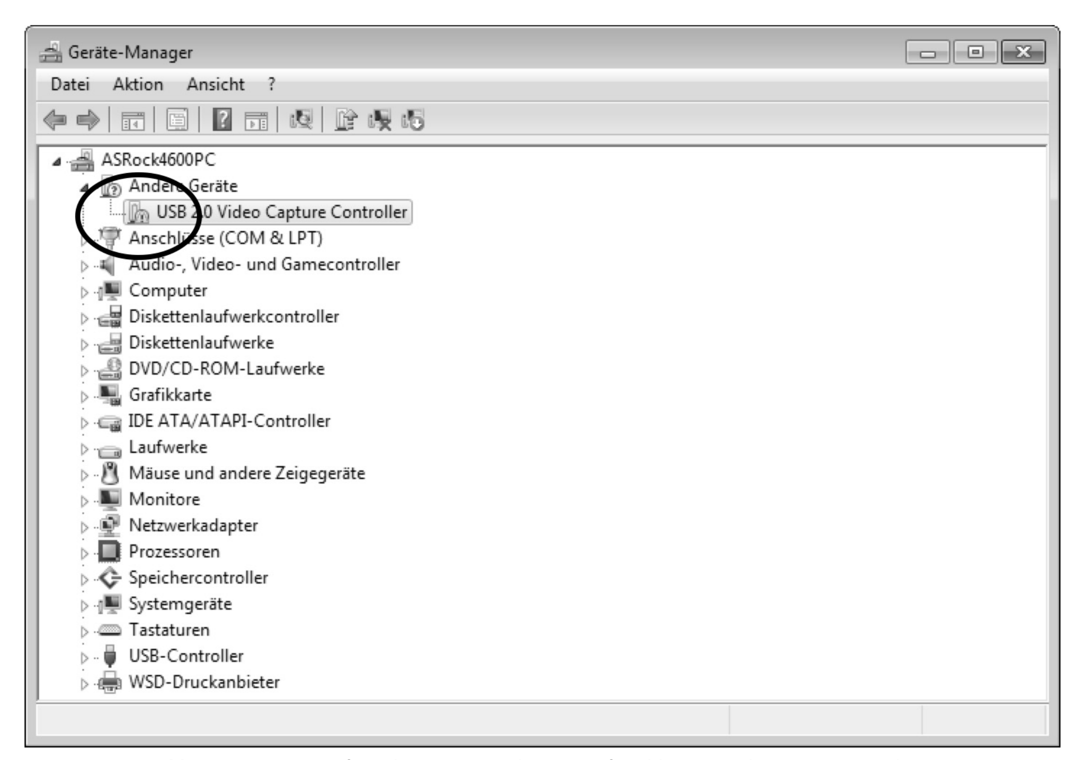


Abb. 6.36: Das Ausrufezeichen im Dreieck weist auf Probleme mit der Komponente hin.

Das Ausrufezeichen ist das weitaus häufigste Fehlersymbol und solche Fehler sind meist einfach zu beseitigen. Zunächst überprüfen Sie noch einmal die Geräteanschlüsse. Dann versuchen Sie, die Treiber erneut zu installieren. Klicken Sie dazu die Komponente mit der rechten Maustaste an und wählen Sie im Kontextmenü TREIBER AKTUALISIEREN (Abbildung 6.37).

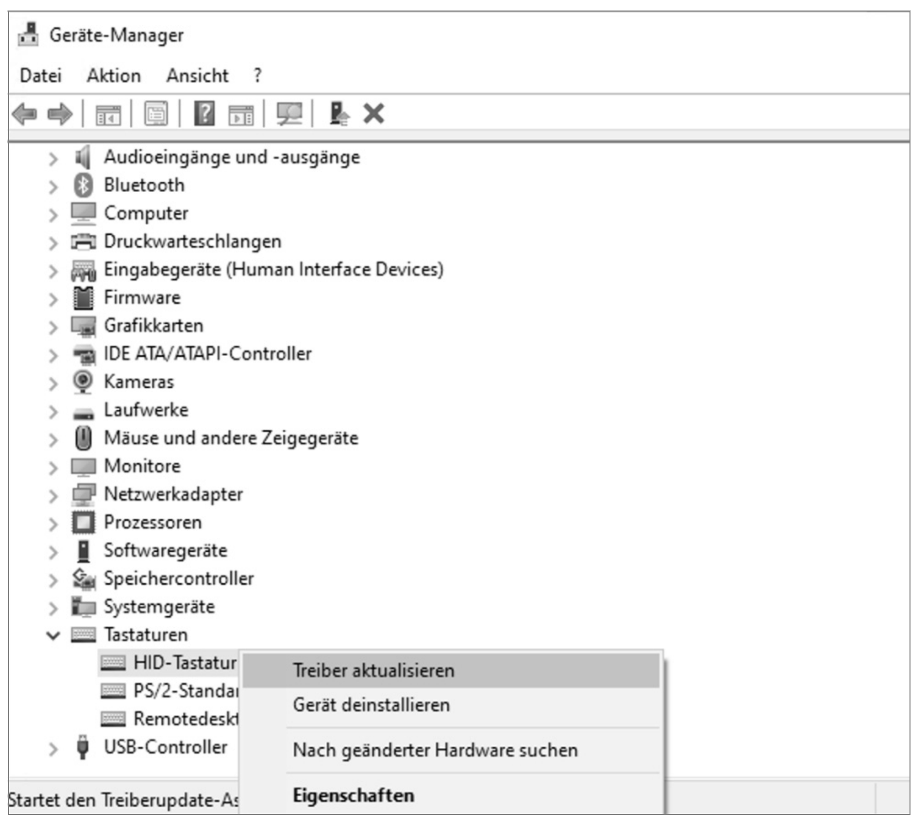


Abb. 6.37: Aktualisieren eines Treibers

Wenn der nach unten weisende Pfeil bei Ihnen auftritt, prüfen Sie zunächst, ob das Gerät nicht deaktiviert ist. Klicken Sie das Gerät mit der rechten Maustaste an und wählen Sie AKTIVIEREN. Sollte das nicht funktionieren (was häufig der Fall ist), versuchen Sie, wieder den zuletzt verwendeten Treiber zu installieren (falls Sie den Treiber aktualisiert haben) oder zu deinstallieren (wenn es sich um eine Neuinstallation handelt). Fahren Sie das System herunter und prüfen Sie, ob die Komponente korrekt installiert ist. Anschließend wiederholen Sie die gesamte Treiberinstallation und achten dabei darauf, möglichst aktuelle Treiber zu verwenden. Wenn keins dieser Verfahren funktioniert, geben Sie die Karte zurück, denn sie ist sehr wahrscheinlich defekt.

6.3 Austausch und Installation eines Mainboards

Viele Techniker werden bei der Frage nach dem Einbau oder Austausch des Mainboards erstaunlich zurückhaltend. Einen Grund dafür gibt es nicht, denn der Einbau eines Mainboards ist eine normale und ziemlich häufige Aufgabe bei der Wartung von Rechnern. Mainboards sind heute vergleichsweise preiswert und lassen sich recht einfach austauschen, auch wenn diese Aufgabe wegen der Vielzahl der Bauteile ihre Tücken hat und ein wenig mühsam sein kann. Dieser Abschnitt beschreibt die Installation bzw. den Ausbau eines Mainboards und zeigt einige Tricks, die Ihnen diese wichtige Aufgabe erleichtern können.

6.3.1 Auswahl von Mainboard und Gehäuse

Die Auswahl von Mainboard und Gehäuse kann sowohl unerfahrene als auch erfahrene Techniker vor gewisse Herausforderungen stellen. Als Erstes müssen Sie festlegen, welchen Typ von Mainboard Sie benötigen, und damit, ob AMD- oder Intel-Prozessoren verwendet werden sollen. Dann müssen Sie sich für einen Formfaktor entscheiden, wobei hier die Art des gewünschten Gehäuses mit in die Entscheidung einfließt. Drittens müssen Sie die vom Mainboard angebotenen Funktionen berücksichtigen und sich überlegen, wie schwierig dessen Konfiguration sein wird. Um hier eine fundierte Entscheidung treffen zu können, müssen Sie das Mainboard-Handbuch lesen! Schließlich müssen Sie dann ein Gehäuse auswählen, das hinsichtlich Platzangebot, Budget und Formfaktor Ihren Anforderungen entspricht. Sehen wir uns also die einzelnen Schritte ein wenig genauer an.

Wichtig

Jeder CompTIA A+-Techniker sollte ein für einen Kunden passendes Mainboard aussuchen und einbauen können.

Stellen Sie als Erstes fest, welches Mainboard benötigt wird. Welcher Prozessor soll verwendet werden? Unterstützt das Mainboard diesen Prozessor? Da meist Prozessor und Mainboard gleichzeitig gekauft werden, lassen Sie sich vom Verkäufer garantieren, dass Prozessor und Mainboard zusammenarbeiten. Wie viel Arbeitsspeicher soll installiert werden? Stehen weitere RAM-Steckplätze für zukünftige Erweiterungen zur Verfügung?

Hinweis

Kapitel 11, *Der maßgeschneiderte PC*, beschäftigt sich näher mit den Komponenten, die für einen spezialisierten PC benötigt werden.

Heute können Sie zwischen einer Reihe hervorragender Mainboard-Anbieter wählen, wie z.B. ASUS, BIOSTAR, GIGABYTE, Intel und MSI. Vielleicht bietet Ihr Händler ja auch weniger bekannte, aber trotzdem erstklassige empfehlenswerte Marken an, von denen Sie eine ausprobieren können.

Zweitens sollte der Formfaktor des Mainboards zu Ihrem Gehäuse passen. Versuchen Sie nicht, ein normales ATX-Mainboard in ein microATX-Gehäuse einzubauen!

Drittens gibt es zu allen Mainboards ein technisches Handbuch, das sogenannte Mainboard-Handbuch (Abbildung 6.38). Dieses Buch müssen Sie unbedingt haben, denn es ist die einzige Informationsquelle für alle kritischen Details im Zusammenhang mit dem Mainboard. Wenn Sie beispielsweise die CPU- oder RAM-Timings im CMOS falsch eingestellt haben und Ihr PC nicht mehr reagiert, wo finden Sie den Jumper zum Löschen des CMOS? Wo wird der Lautsprecher angeschlossen? Auch wenn Sie diese Arbeiten vielleicht nicht selber ausführen, sollten Sie beim Kauf immer auf dem Mainboard-Handbuch bestehen, denn irgendwann werden Sie es benötigen!

Hinweis

Wenn Ihnen bei einem Mainboard das Handbuch fehlt, dann erhalten Sie es meist online als PDF-Dokument auf der Website des Herstellers. In solch einem Fall wäre es auch nicht schlecht, wenn Sie es dann ausdrucken und zusammen mit dem Mainboard aufbewahren würden. Ich klebe häufig eine Kopie des Handbuchs (entweder als Ausdruck, auf CD gebrannt oder auf einen USB-Stick kopiert) in das Gehäuse, in das ich das Mainboard installiert habe. Achten Sie jedoch darauf, nicht versehentlich Lüftungsschlitze abzudecken.



Abb. 6.38: Karton und Handbuch eines Mainboards

Tipp: Aufbau eines guten Rufs

Familienmitglieder, Freunde und potenzielle Kunden suchen häufig den Rat eines Technikers, wenn sie darüber nachdenken, ihren PC aufzurüsten. Bei solch einem Ansuchen sollten Sie nicht nur eine Empfehlung aussprechen können, sondern auch die Bedürfnisse und das Budget des Ratsuchenden berücksichtigen. Sie müssen den Erwartungen gerecht werden und die richtigen Fragen stellen!

Welche Aufgaben möchte der Benutzer mit dem aufgerüsteten System erledigen? Notieren Sie sich das! Oft geht es darum, dieses tolle neue Spiel nutzen zu können oder eine neue Technologie einzusetzen. Welche minimalen Systemanforderungen muss der Rechner erfüllen, um auch in einem halben Jahr noch ausreichend leistungsfähig für neue Spiele zu sein? Welche Ausstattung ist für vernünftige Multimediaanwendungen erforderlich? Sollte das Mainboard über SuperSpeed USB 3.0 oder SuperSpeed+ USB 3.1 verfügen, um beispielsweise Videobearbeitung oder eine andere spezielle Anwendung zu ermöglichen?

Welche Komponenten des bisherigen Systems möchte der Benutzer weiterhin verwenden? Ein neues Mainboard kann schnell dazu führen, dass das gesamte System neu aufgebaut werden muss. Welchen Formfaktor besitzt das alte Gehäuse? Falls es ein microATX-Gehäuse ist, sind Sie bei der Auswahl auf Mainboards dieser Größe eingeschränkt. Wenn ein Mainboard in ATX-Größe erwünscht ist, müssen Sie ein neues Gehäuse beschaffen. Ist der Sockel des neuen Mainboards vom gleichen Typ wie derjenige des alten? Falls nicht, ist auch ein neuer Prozessor fällig.

Und wie sieht es mit RAM aus? Wenn das alte Mainboard DDR3-SDRAM verwendet und für das neue DDR4-SDRAM erforderlich ist, muss das RAM ebenfalls ersetzt werden. Sie sollten wissen, wie viele Kanäle das neue RAM unterstützt, da die Leistung am besten ist, wenn alle Kanäle genutzt werden.

Sobald Sie diese Informationen gesammelt haben und den aktuellen PC des Benutzers beurteilen können, ist es Zeit für einen Einkaufsbummel! Das gibt Ihnen auch Gelegenheit, sich beim Computerhändler nach den neuesten Mainboards und anderem Zubehör umzusehen. Vergessen Sie dabei nicht, sich Notizen zu machen und die Preise aufzuschreiben. Am Ende des Einkaufsbummels sollten Sie über hinreichende Informationen verfügen, um dem Benutzer eine ehrliche Einschätzung zu geben, was mit der Aufrüstung des PCs auf ihn zukommt, zumindest in finanzieller Hinsicht. Seien Sie dabei aufrichtig und erzählen Sie dem Benutzer nicht das, was er vielleicht gerne hören möchte – dann kann es auch nicht zu Schwierigkeiten kommen.

Wählen Sie viertens das Gehäuse sorgfältig aus. Gehäuse werden in vielen Varianten angeboten: Slimline, Desktop, Mini-Tower, Midi-Tower, Tower und Cube. Außerdem gibt es spezielle Gehäuse, die in der Formgebung an andere Geräte der Unterhaltungselektronik angepasst sind (wie etwa Hi-Fi-Anlage oder DVD-Spieler). Die CompTIA spricht hier von *HTPC*-Gehäusen (*Home Theater PC*). Abbildung 6.39 zeigt ein solches Gehäuse.



Abb. 6.39: Ein HTPC-Gehäuse

Slimline- und Desktop-Gehäuse werden normalerweise auf dem Schreibtisch unter den Monitor gestellt. Die verschiedenen Tower-Varianten beanspruchen in der Nähe des Schreibtischs ein wenig Platz auf dem Fußboden. Heute werden vorwiegend Mini- und Midi-Tower verwendet. Überzeugen Sie sich davon, dass das Gehäuse zum Mainboard passt. Viele micro- und FlexATX-Gehäuse sind einfach zu klein für normale ATX-Mainboards. Für Cube-Gehäuse benötigen Sie im Allgemeinen ein besonderes Mainboard, deshalb sollten Sie darauf achten, beide Bauteile gleichzeitig zu kaufen. Eine kurze Prüfung vor dem Kauf kann Ihnen hier viel Lauferei ersparen.

Bei besseren Gehäusen ist es möglich, Komponenten ohne Werkzeug einzubauen. Karten und Laufwerke müssen nicht verschraubt werden, sondern rasten einfach ein. Zum Festschrauben des Mainboards benötigen Sie dennoch einen Schraubendreher. Ganz ohne Werkzeug geht es eben doch noch nicht.

Netzteile werden häufig zusammen mit dem Gehäuse angeboten. Hüten Sie sich vor Gehäuse-Supersonderangeboten, weil diese häufig auf billige oder fehlende Netzteile hinweisen. Außerdem müssen Sie darauf achten, dass das Netzteil ausreichend Leistung bietet. Diese Aspekte werden in Kapitel 7, *Netzteile*, eingehender beleuchtet.

6.3.2 Installation eines Mainboards

Wenn Sie ein Mainboard auswechseln müssen, bauen Sie als Erstes das alte Mainboard aus. Entfernen Sie zu diesem Zweck erst einmal alle Steckkarten. Entfernen Sie außerdem alles, was den Ausbau oder die Installation des Mainboards behindern könnte, wie z.B. Festplatten. Achten Sie auf die Schrauben – am besten drehen Sie die Schrauben nach dem Ausbau der Komponenten vorübergehend wieder in die Schraublöcher ein, bis Sie diese erneut zum Einbau benötigen. Manchmal muss man vorübergehend auch das Netzteil ausbauen, um an das Mainboard heranzukommen.

Wichtig

Die CompTIA A+-Prüfung fragt ab, ob Sie ein Mainboard einbauen können, lesen Sie diesen Abschnitt also sorgfältig durch!

Lösen Sie die Schrauben des Mainboards. *Das Mainboard lässt sich oft nicht einfach herausheben*, da es mit kleinen *Abstandhaltern* im Gehäuse befestigt ist, die seitlich in Aussparungen im Gehäuse geschoben

werden und dort einrasten (Abbildung 6.40). In die Distanzbolzen aus Metall (*Standouts*) werden Schrauben gedreht, die das Mainboard in Position halten. Sorgen Sie vor der Installation des neuen Mainboards dafür, dass die Distanzbolzen korrekt ausgerichtet sind.

Vorsicht

Vermeiden Sie hier elektrostatische Entladungen (ESD)! Denken Sie daran, dass Prozessoren und RAM-Module durch elektrostatische Entladungen leicht zerstört werden können. Und auch das Mainboard kann dadurch leicht beschädigt werden. Tragen Sie Ihr Antistatikarmband!

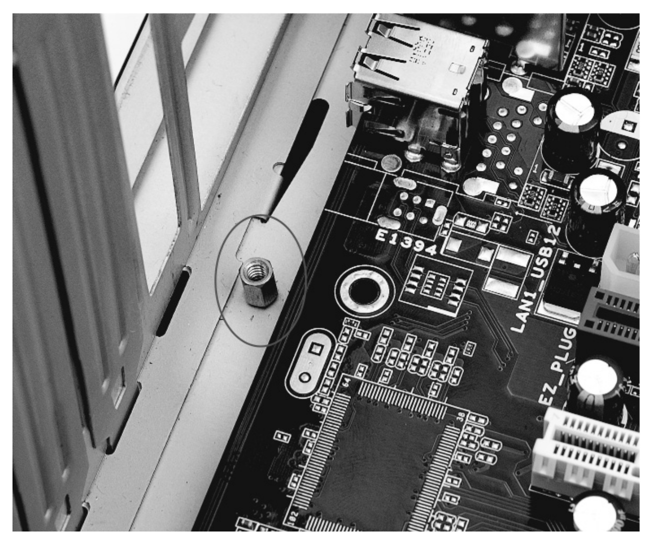


Abb. 6.40: Distanzbolzen im Gehäuse vor dem Einbau des Mainboards

Beim Einbau des neuen Mainboards sollten Sie nicht unbedingt davon ausgehen, dass die Schrauben und Abstandhalter wieder an derselben Stelle eingebaut werden. Folgen Sie hinsichtlich der Schrauben und Abstandhalter stattdessen der Regel: Wenn es passt, dann passt es! An dieser Stelle sollten Sie nicht allzu ängstlich sein, denn der Einbau eines Mainboards kann manchmal ein etwas energischeres Vorgehen erfordern! Hier müssen Sie ein wenig drücken, dort ein wenig wackeln, und wenn Sie Pech haben, können Sie sich dabei auch ein wenig Haut abschürfen.

Vorsicht

Achten Sie beim Austausch des Mainboards auf die Position der Distanzstücke. Wenn Sie einen Distanzbolzen aus Metall an einer Stelle des Mainboards zu entfernen vergessen, an der es keine entsprechende Bohrung gibt und das Mainboard dann mit Strom versorgen, dann riskieren Sie Kurzschlüsse.

Der nächste Schritt bei der Mainboard-Installation ist der Anschluss der LED-Anzeigen, der Schalter und der zum Frontpanel des Gehäuses führenden Kabel. Oftmals lässt sich das einfacher erledigen, wenn das Mainboard noch nicht vollständig ins Gehäuse eingebaut ist. Sie können dem Verlauf der Kabel von der Vorderseite des Gehäuses zu den jeweiligen Anschlüssen dann besser folgen. Dazu gehören normalerweise:

- Softpower
- Reset-Taste

- Lautsprecher
- Festplatten-LED
- Betriebsanzeige-LED
- USB
- Sound
- Thunderbolt

Alle diese Kabel verfügen über spezielle Anschlusspins auf dem Mainboard. Erfahrene Techniker brauchen meist nur kurz das Mainboard zu betrachten, um die Position dieser Pins zu ermitteln (Abbildung 6.41). Sie ist aber auch im Mainboard-Handbuch dokumentiert.

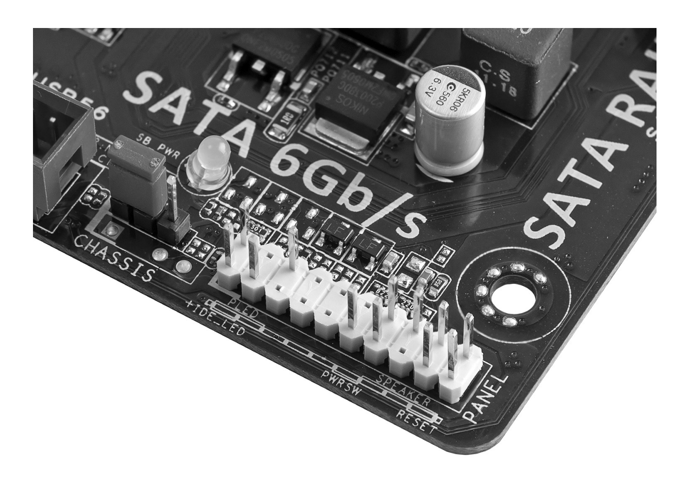


Abb. 6.41: Die Funktion der Anschlusspins ist hier auf dem Mainboard angegeben

Hinweis

Viele Techniker installieren den Prozessor, seinen Lüfter und den Arbeitsspeicher auf dem Mainboard, bevor sie dieses in das Gehäuse einbauen. Dadurch erleichtern Sie sich – speziell bei einem neuen System – die Arbeit. Erstens wollen Sie wissen, ob Prozessor und Speichermodule mit dem Mainboard zusammenarbeiten, da sich ansonsten kein stabiles System einrichten lässt. Zweitens lässt sich auf diese Weise das Durchbiegen des Mainboards verhindern. Einige Gehäuse stützen das Mainboard nur unzureichend, sodass es z.B. beim Einsetzen der Speicherbausteine durchgebogen wird, wodurch Leiterbahnen brechen könnten. Drittens ist das Anbringen des Lüfters häufig extrem schwierig, wenn das Mainboard bereits im Gehäuse eingebaut ist, und wird viel einfacher, wenn die Platine auf einer Tischplatte liegt. Viele Kühlbaugruppen von Drittherstellern werden mit Klammern am Mainboards befestigt, die installiert werden müssen, bevor das Mainboard eingesetzt wird.

Beim Anschluss dieser Kabel sollten Sie einige Regeln befolgen. Die erste Regel lautet: »LED-Lämpchen sind keine Glühbirnen – sie besitzen einen positiven und negativen Pol.« Falls sie nicht funktionieren, sollten Sie daher die Anschlüsse vertauschen und sehen, ob sie nun leuchten. Die zweite Regel lautet: »Wenn Sie mal im Unklaren sind, raten Sie einfach!« Falsche Verbindungen haben hier keine Beschädigung des Rechners zur Folge. Das falsch angeschlossene Bauteil funktioniert dann nur nicht. Hinweise für den korrekten Anschluss finden Sie im Mainboard-Handbuch. Die dritte und letzte Regel lautet: »Außer *Softpower* wird bei ATX-Systemen kein weiterer Anschluss benötigt, um den Rechner in Betrieb nehmen zu können!«

Es gibt keine einfachen und festen Regeln zum Identifizieren der Funktion der einzelnen Kabel. Häufig befinden sich auf den kleinen Anschlusssteckern aufgedruckte Hinweise (Abbildung 6.42). Falls

nicht, müssen Sie den Verlauf der Leitungen zum Gehäuse (z.B. zu den LEDs oder Schaltern) einzeln verfolgen, um ihre Funktion zu ermitteln.

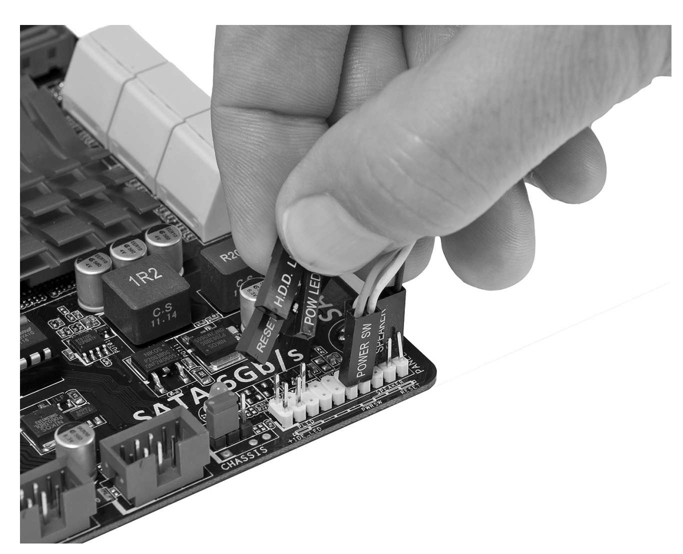


Abb. 6.42: Ein Beispiel für die Leitungen zum Gehäuse

Befestigen Sie das Mainboard nun mit den entsprechenden Schrauben und verbinden Sie alle Kabel. Sobald Sie das Mainboard in das Gehäuse eingebaut und CPU und RAM korrekt installiert sind, sollten Sie die Stromversorgung herstellen und anfangen zu testen. Eine POST-Karte kann hier sinnvoll sein, da der Systemtest zur Überprüfung des Bootvorgangs vorerst noch ohne Lautsprecher, Grafikkarte, Monitor und Tastatur auskommen muss. Falls Sie eine POST-Karte besitzen, starten Sie das System und überzeugen Sie sich davon, dass der POST ausgeführt wird. Die Karte zeigt dann eine Reihe von POST-Zahlencodes an, die an einer bestimmten Stelle stoppen. Wenn Sie keine POST-Karte haben, schließen Sie Tastatur, Lautsprecher, Grafikkarte und Monitor an. Booten Sie das System und schauen Sie, ob die BIOS-Informationen auf dem Bildschirm angezeigt werden. Wenn ja, gibt es wahrscheinlich keine Probleme. Wenn nicht, schauen Sie im Mainboard-Handbuch nach, wo Sie einen Fehler begangen haben könnten.

Falls das Mainboard überhaupt keine elektrische Spannung erhält, überprüfen Sie die Kabelverbindungen aller erforderlichen Anschlüsse. Falls die Lüfter laufen, aber der Bildschirm leer bleibt, kann das verschiedene Ursachen haben. Vielleicht ist die CPU, ein Speichermodul oder die Grafikkarte nicht korrekt mit dem Mainboard verbunden. Die einzige Möglichkeit, das herauszufinden, sind Tests. Überprüfen Sie zunächst die einfachen Verbindungen (RAM und Grafikkarte), bevor Sie die CPU entfernen und erneut einsetzen. Lesen Sie bei Problemen mit der Stromversorgung auch in Kapitel 7, *Netzteile*, nach.

Wichtig

Bei sehr alten Mainboards musste die Geschwindigkeit des Systembusses mittels kleiner Steckbrücken oder Jumpern eingestellt werden. Dadurch war es möglich, diese Mainboards an eine CPU anzupassen, die beispielsweise einen 100-MHz- oder einen 66-MHz-Bus benötigt. In der CompTIA A+-Prüfung könnte diese manuelle Einstellung abgefragt werden.

Wenn man dabei einen Fehler machte, führte das zu seltsamen Verhalten. Wenn die Busgeschwindigkeit zu hoch war, starteten viele CPUs überhaupt nicht. War sie zu gering, wurde die CPU nicht optimal genutzt. In den Mainboard-Handbüchern gab es umfangreiche Diagramme mit den Einstellungen für unterstützte CPUs.

Moderne Mainboards können CPU- und RAM-Einstellungen automatisch ermitteln und passen die Einstellungen dementsprechend an. Derartige Fehler können also nur noch auftreten, wenn Sie die CPU mit dem CMOS-Setup-Programm absichtlich über- oder untertakten.

6.4 Problembehebung bei Mainboards

Mainboards fallen gelegentlich aus. Das geschieht zwar nicht gerade häufig, aber Mainboards und deren Komponenten können aus vielen Gründen versagen: Alter, Staub, Tierhaare oder kleine Fertigungsfehler und die durch die Leiterbahnen geleiteten Ströme führen mit der Zeit zu Defekten. Mainboards können aber auch Schaden nehmen, wenn einmal zu viel Erweiterungskarten eingebaut werden, sei es nun durch elektrostatische Entladungen oder dadurch, dass beim Einsetzen von Steckkarten oder Speichermodulen das Mainboard zu stark durchgebogen wird. Das Mainboard ist eine schwer arbeitende, häufig viel zu wenig beachtete PC-Komponente! Leider kann die Fehlersuche bei Mainboard-Problemen schnell schwierig und zeitaufwendig werden. Schließen wir dieses Kapitel also mit einer Betrachtung der Symptome ausfallender Mainboards, Techniken der Problembehebung und der verfügbaren Optionen bei auftretenden Mainboard-Problemen ab.

Tipp

Zu Kapitel 6 gibt es unter `http://totalsem.com/100x` eine Übung, die Ihnen dabei hilft, die Komponenten eines Mainboards zu erkennen, für den Fall, dass Sie in der CompTIA A+-Prüfung eine Frage dazu beantworten müssen.

6.4.1 Symptome

Mainboard-Fehler lassen sich drei Kategorien zuordnen: Totalausfall, Ausfall einzelner integrierter Komponenten und »Spuk«. Beim *Totalausfall* bootet der Rechner einfach nicht mehr. Wenn ein eben noch funktionierender PC plötzlich komplett ausfällt, nachdem Sie einen Knall – ein lautes Geräusch – gehört haben und dann den stechenden Geruch von Ozon wahrnehmen, dann ist der Computer abgeraucht. Versuchen Sie zu erschnüffeln, ob es einen geplatzten Kondensator oder ein anderes defektes Bauteil auf dem Mainboard gibt. Überprüfen Sie die Spannungsversorgung und die Betriebsanzeige der Festplatte. Wenn vorher alles funktioniert hat, weist das auf ein defektes Netzteil oder Mainboard hin.

Diese Art von Problemen tritt vergleichsweise häufig bei nahezu neuen Systemen (aufgrund unerkannter Fertigungsfehler) oder bei Systemen auf, die einer elektrostatischen Entladung ausgesetzt waren. Die Fehler bei neuen Systemen (sogenannte *Burn-in-Fehler*) sind hier wiederum relativ selten und treten üblicherweise innerhalb der ersten 30 Tage der Benutzung auf. Wenn Sie dann das Mainboard ersetzen, sollte damit das Problem behoben sein. Wenn Sie dem Mainboard versehentlich beim Einsetzen einer Steckkarte oder dem Anschluss von Kabeln eine ordentliche elektrostatische Ladung verpassen, dann haben Sie guten Grund, sich zu ärgern. Vielleicht gewöhnen Sie es sich dann aber endlich ab, ohne Antistatikarmband zu arbeiten!

Wichtig

Mitte der 2000er-Jahre lieferten die Hersteller von Kondensatoren einige Jahre lang zum Teil defekte Bauteile aus. (Kondensatoren speichern elektrische Energie und geben diese wieder ab. Sie werden vor allem zur Spannungsglättung für Mainboards und andere gedruckte Schaltungen eingesetzt.) Millionen dieser fehlerhaft gefertigten Kondensatoren wurden in Computern verbaut und viele dieser Bauteile fielen aus. Die angeschwollenen oder sogar aufgeplatzten Kondensatoren wiederum führten zu »toten« PCs. Sie können in der CompTIA A+-Prüfung 1001 ebenfalls vorkommen.

Integrierte Komponenten fallen ebenfalls nur selten aus. Derartige Fehler werden aber gelegentlich durch Wackelkontakte zwischen einer Komponente und dem Mainboard verursacht oder treten unregelmäßig auf. Wenn eine Festplatte z.B. an einen fehlerhaften Controller auf dem Mainboard angeschlossen ist, dann wird sie zwar möglicherweise vom CMOS automatisch erkannt, Windows kann aber nicht darauf zugreifen. Ein weiteres Beispiel ist ein USB-Anschluss, der lange tadellos funktioniert hat, bis z.B. Überspannungen bei einem Unwetter für das Ende des daran angeschlossenen externen Modems und des USB-Anschlusses gesorgt haben, der nun auch mit einem neuen Modem nicht mehr funktioniert.

Am schwierigsten von den drei Symptomarten lassen sich jene diagnostizieren, bei denen es im System scheinbar spukt. Komponenten funktionieren hier und da nicht, der PC führt offenbar grundlos von selbst einen Neustart durch. Mitten während der Arbeit wird plötzlich ein blauer Bildschirm angezeigt und das gerade, kurz bevor Sie den Schurken erschlagen und die holde Maid retten konnten. Was kann derartige Symptome verursachen? Wenn Sie jetzt irgendeine der nachfolgenden Ursachen genannt hätten, dann lägen Sie richtig:

- Fehlerhafte Komponenten
- Fehlerhafte Gerätetreiber
- Fehlerhafte Anwendungsprogramme
- Einzelne beschädigte Betriebssystemdateien
- Probleme des Netzteils

Nun ja, Sie haben schon verstanden ...

Ein Albtraum, was die Problembehebung betrifft! Wie Techniker hier Durchblick bewahren und welche Verfahren zur Problembehebung sie dabei anwenden, sollen Sie nun erfahren.

6.4.2 Techniken der Problembehebung

Wenn es um ein potenziell defektes Mainboard geht, dann sind Zeit, Geduld und Organisationstalent gefragt. Einige Probleme lassen sich sicherlich schneller erkennen als andere. Wenn die Festplatte wie im letzten Beispiel nicht wie erwartet funktioniert, dann prüfen Sie die Einstellungen am Laufwerk. Probieren Sie ein anderes Laufwerk aus. Probieren Sie dasselbe Laufwerk an einem anderen Mainboard aus, um sich davon zu überzeugen, dass es fehlerfrei funktioniert. Wie bei allen anderen Techniken zur Problembehebung führen Sie auch beim Mainboard Tests aus, um das Problem zu isolieren und mögliche Ursachen zu eliminieren. Verwenden Sie eine moderne POST-Karte mit vernünftiger Anzeige. Es gibt derartige Karten, die sowohl an PCI- als auch an PCIe-Steckplätze anschließbar sind. Es sind sogar POST-Karten für den USB-Anschluss erhältlich, die eine schnelle Diagnose tragbarer Computer ermöglichen (Abbildung 6.43).

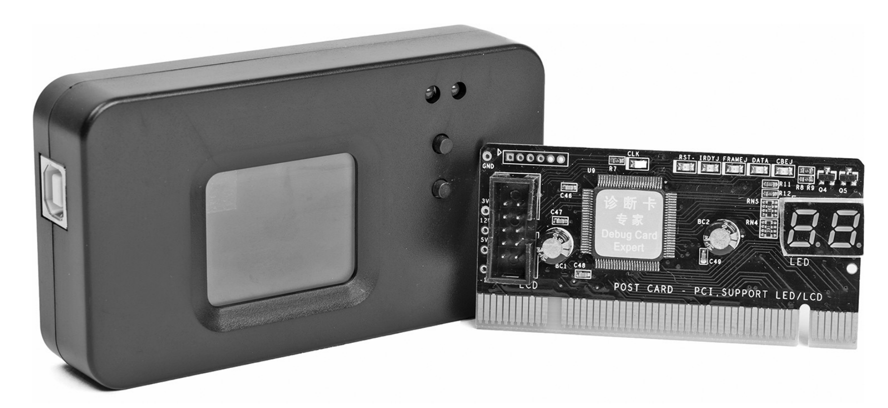


Abb. 6.43: POST-Karten für den USB-Anschluss (links) und den PCI-Steckplatz (rechts)

Diese drei Schritte der Systemprüfung, des Austauschens und der Prüfung, ob Komponenten fehlerfrei funktionieren, eignen sich für einfachere und komplexe Mainboard-Probleme. Sie können diese Technik sogar für Probleme einsetzen, bei denen es im System zu spuken scheint und die Ursache überall liegen könnte, aber dann sollten Sie alle Aktionen ausführlich *dokumentieren*. Machen Sie sich Notizen zu den einzelnen, getesteten Komponenten, damit Sie die Tests nicht unnötig wiederholen oder nutzlos Zeit verschwenden. Darüber hinaus lassen sich so vielleicht gewisse Fehlermuster erkennen. Wenn Sie einen Systemabsturz dadurch reproduzieren können, dass Sie bestimmte Maßnahmen in einer bestimmten Reihenfolge ausführen, dann offenbart Ihnen das häufig die eigentliche Ursache des Problems. Das Testen von Mainboards kostet bereits ohne überflüssige, ineffiziente Anstrengungen genug Zeit!

6.4.3 Optionen

Wenn Sie festgestellt haben, dass das Mainboard die Probleme verursacht, dann haben Sie mehrere Optionen zur Behebung der drei Fehlervarianten. Handelt es sich um größere Schäden, dann müssen Sie das Mainboard austauschen. Auch wenn Teile noch funktionieren, sollten Sie das Problem nicht leichtfertig handhaben. Das Mainboard sollte die Stabilität des Systems in keiner Weise beeinträchtigen. Auch wenn es nur ansatzweise Fehler oder Probleme zeigt, sollten Sie es loswerden!

Wenn eine der integrierten Komponenten ausfällt, dann können Sie diese häufig durch eine Zusatzkarte mit denselben oder umfassenderen Funktionen ersetzen. Adaptec stellt z.B. Steckkarten her, mit denen sich die integrierten SATA-Anschlüsse auf dem Mainboard ersetzen lassen (Abbildung 6.44).

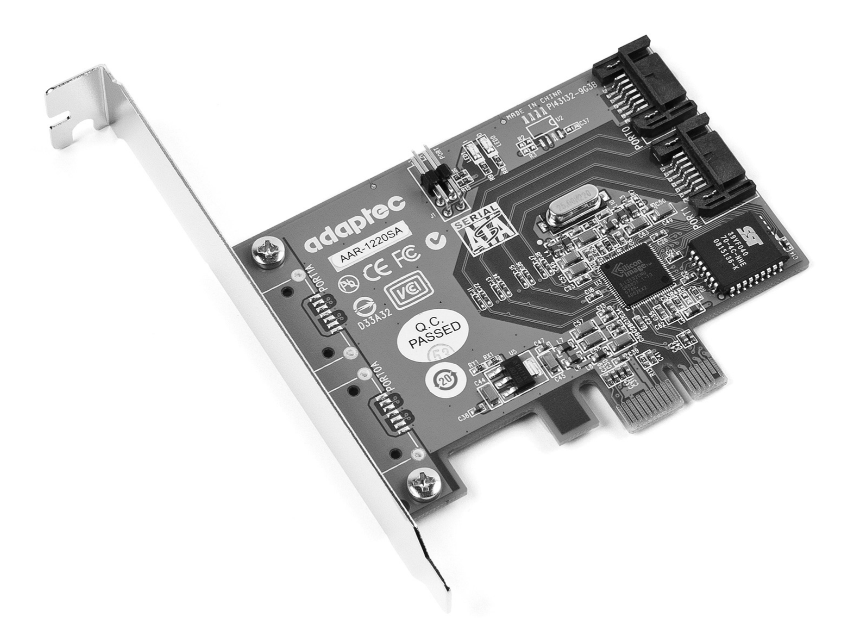


Abb. 6.44: SATA-Controller der Firma Adaptec für den PCIe-Steckplatz

Wenn die Komponenten aus technischen Gründen und nicht aufgrund physischer Beschädigungen ausfallen, dann können Sie versuchen, das Mainboard-BIOS zu aktualisieren. Aus Kapitel 5, *BIOS und CMOS*, wissen Sie, dass alle Mainboards über Programme verfügen, durch die der Prozessor mit den in das Mainboard integrierten Komponenten kommunizieren kann. Diese BIOS-Programme lassen sich bei modernen Mainboards vergleichsweise einfach aktualisieren (flashen). Um das neue BIOS in den Flash-ROM-Chip zu schreiben, müssen Sie nur ein kleines Programm ausführen. In Kapitel 5, *BIOS und CMOS*, erfahren Sie, wie Sie bei der BIOS-Aktualisierung vorgehen müssen.

Hinweis

Durch das Flashen des Mainboard-BIOS lassen sich manchmal eine ganze Reihe von Problemen beheben, die sich negativ auf die Systemstabilität auswirken. Zudem wird die in das Mainboard integrierte Technologie oft besser unterstützt. Für bessere Systemhardware kann eine BIOS-Aktualisierung allerdings nicht sorgen. Wenn AMD z.B. einen neuen, verbesserten Prozessor der A-Reihe vorstellt, der mit niedrigerer Spannung auskommt, die vom Mainboard nicht unterstützt wird, dann lässt sich dieser Prozessor nicht verwenden, selbst wenn er in den auf dem Mainboard vorhandenen AM4-Sockel passt. Sie können das BIOS so oft aktualisieren, wie Sie wollen, die Hardware auf dem Mainboard bleibt dieselbe.

Sollte es sich schließlich um ein Problem handeln, bei dem es im System scheinbar spukt und das mit dem Mainboard im Zusammenhang steht, dann gibt es nur wenige Optionen zur Behebung des Problems. Sie können das BIOS in einem verzweifelten Versuch, den Fehler zu beheben, neu programmieren (flashen). Manchmal lassen sich Probleme dadurch beheben. Jedenfalls ist diese Option preiswerter als die andere Alternative, das Ersetzen des Mainboards.

6.5 Wiederholung

6.5.1 Fragen

1. Welcher der folgenden Aussagen über den Erweiterungsbus trifft zu?
   A. Der Erweiterungsbus läuft mit der Geschwindigkeit des Systemtakts.
   B. Der Taktgeber des Erweiterungsbusses legt dessen Geschwindigkeit fest.
   C. Die CPU kommuniziert über den Erweiterungsbus mit dem RAM.
   D. »Frontside-Bus« ist eine andere Bezeichnung dafür.
2. Was bedeutet ein schwarzer, nach unten weisender Pfeil neben einer Komponente im Geräte-Manager?
   A. Es wurde ein kompatibler Treiber installiert, der möglicherweise nicht alle Funktionen der Komponente unterstützt.
   B. Die Komponente ist nicht vorhanden oder kann von Windows nicht erkannt werden.
   C. Die Systemressourcen wurden manuell zugewiesen.
   D. Das Gerät wurde deaktiviert.
3. Welche PCI-Variante wurde speziell für Laptops entwickelt?
   A. PC-X
   B. PCIe
   C. Mini-PCI
   D. AGP
4. Welcher der folgenden Formfaktoren wird bei modernen PCs vorwiegend verwendet?
   A. AT
   B. ATX
   C. ITX
   D. BTX
5. Anna hat ein neues System gekauft, das mitten in einer wichtigen Präsentation einen Blue Screen of Death angezeigt hat. Danach bootete das System überhaupt nicht mehr, nicht einmal ins CMOS. Nach ausführlicher Fehlersuche stellt sie fest, dass das Mainboard defekt ist, und tauscht es aus. Jetzt läuft das System ausgezeichnet. Was war die wahrscheinlichste Ursache des Problems?
   A. Burn-in-Fehler
   B. Elektrostatische Entladung

   C. Komponentenausfall
   D. Netzteilfehler

6. Martin hat ein neues Mainboard gekauft, das sein altes ATX-Mainboard ersetzen soll. Als er den Laden verlässt, ruft ihm der Verkäufer hinterher: »Und achten Sie auf Ihre Distanzstücke!« Was könnte er damit gemeint haben?
   A. Distanzstücke sind die Anschlüsse am Mainboard für die Tasten an der Vorderseite, wie beispielsweise Netzschalter und Reset-Taste.
   B. Distanzstücke sind die Metallkanten an einigen Gehäusen, die nicht abgerundet sind.
   C. Distanzstücke sind die Metallbolzen, über die das Mainboard im Gehäuse befestigt wird.
   D. Distanzstücke sind Slotbleche, über die ein Mainboard mehr als vier USB-Anschlüsse unterstützen kann.
7. Wilfried hat einen sehr fehlerhaften Rechner, der ständig abstürzt und spontan neu startet. Er verdächtigt das Mainboard. Wie kann er es testen?
   A. Er überprüft die Einstellungen und probiert bekanntermaßen fehlerfreie Komponenten aus.
   B. Er ermittelt, welche Komponenten korrekt funktionieren, und dokumentiert seine Tests.
   C. Er tauscht als Erstes das Mainboard aus, um zu prüfen, ob das Problem damit verschwindet.
   D. Er überprüft die Einstellungen, ermittelt, welche Komponenten korrekt funktionieren, tauscht Komponenten aus und dokumentiert seine Tests.
8. Als Julia stolz ihr neues Mainboard vorführt, kratzt sich der Cheftechniker am Kopf und fragt: »Und was für eine Northbridge hat es?« Wonach fragt er wohl?
   A. Nach dem PCI-Steckplatz
   B. Nach dem PCIe-Steckplatz
   C. Nach dem Chipsatz
   D. Nach dem USB-Controller
9. Welche Unternehmen dominieren den Markt bei Chipsätzen? (Wählen Sie zwei Antworten aus.)
   A. AMD
   B. Intel
   C. NVIDIA
   D. SiS
10. Wenn Windows ein Gerät erkennt, wo erscheint es dann?
   A. Im Geräte-Manager
   B. Unter `C:\Windows\System32\Devices`
   C. Auf dem Desktop
   D. Im Applet HARDWARE SICHER ENTFERNEN

6.5.2 Antworten

1. **B.** Ein separater Taktgeber sorgt dafür, dass der Erweiterungsbus mit einer anderen Geschwindigkeit als der Frontside-Bus arbeiten kann.
2. **D.** Das Gerät wurde deaktiviert.
3. **C.** Das Mini-PCI-Format spart Platz und Strom, wodurch es zum idealen Kartentyp für Laptops wird.
4. **B.** Fast alle modernen Mainboards entsprechen dem ATX-Formfaktor.
5. **A.** Obwohl alle Antworten plausibel sind, lautet die beste Antwort hier, dass beim System ein Burn-in-Fehler aufgetreten ist.

6. **C.** Distanzstücke sind die Metallbolzen, über die das Mainboard im Gehäuse befestigt wird.
7. **D.** Wilfried muss die Einstellungen prüfen, feststellen, welche Komponenten korrekt funktionieren, Komponenten austauschen und alle Tests dokumentieren.
8. **C.** Der Techniker verwendet alte Terminologie für den Chip bzw. den Chipsatz, der die CPU bei der Kommunikation mit Geräten unterstützt.
9. **A, B.** AMD und Intel stellen die allermeisten der in modernen PCs verwendeten Chipsätze her.
10. **A.** Windows zeigt erkannte Geräte im Geräte-Manager an.

Netzteile 7

Themen in diesem Kapitel:

- Grundlagen der Elektrizität und der Elektrotechnik
- Stromversorgung des PCs
- Netzteile einbauen, warten und prüfen
- Fehlersuche bei Netzteilen und Brandschutz

Computer benötigen Strom. Wo der herkommt, hängt vom Gerät ab. Mobile Geräte verwenden Akkus (siehe Kapitel 23, *Tragbare Computer*). Für die Stromversorgung eines Desktop-Rechners sorgt üblicherweise ein einziges Kästchen, das Netzteil, das mit einer Steckdose verbunden wird und den Strom so umwandelt, dass er sich für den Betrieb des Computers eignet. Abbildung 7.1 zeigt ein typisches Netzteil in einem Gehäuse.



Abb. 7.1: Ein typisches Netzteil, das im Rechnergehäuse montiert wird

Oberflächlich betrachtet scheint dies recht einfach zu sein. Die verschiedenen Aspekte im Zusammenhang mit Netzteilen sind für Techniker aber von kritischer Bedeutung. Probleme der Stromversorgung können zu Systeminstabilität, Abstürzen und Datenverlust führen, durchweg Folgen, die es zu vermeiden gilt! Gute Techniker wissen daher eine ganze Menge über die Stromversorgung des Rechners und kennen die Grundlagen der Elektrizität und der Elektrotechnik sowie die vielen Netzteilvarianten. Zudem müssen sie Probleme der Stromversorgung erkennen und geeignete Lösungen einrichten können. Zu viele Techniker sagen achselzuckend »Schließen Sie es einfach an«, und wissen zum Leidwesen ihrer Kunden nicht, wie mit Problemen bei der Stromversorgung umzugehen ist.

Wichtig

Einige Fragen in den CompTIA A+-Zertifizierungsprüfungen könnten sich auf Netzteile beziehen, die auch *PSU* (*Power Supply Unit*) genannt werden. Ein Netzteil fällt außerdem in die Kategorie der typischen *Ersatzteile* (*FRU, Field Replaceable Unit*), die ein Techniker bei sich haben sollte, ebenso wie Speichermodule und eine Festplatte.

Geschichte und Konzepte

7.1 Grundlagen der Elektrizität

Mit Elektrizität ist grundsätzlich einfach ein Fluss negativ geladener Teilchen, der *Elektronen*, durch Materie gemeint. Der Fluss der Elektronen wird von den verschiedenen Materialien unterschiedlich stark unterstützt. Dieser Elektronenfluss ist vergleichbar mit Wasser, das durch Rohre fließt. Am besten stellen Sie sich bei der Betrachtung der Elektrizität Wasser vor, das durch Rohre fließt! Unterhalten wir uns also einen Moment lang über Wasser.

Wasser kommt aus dem Boden, aus Brunnen, aus Quellen, fließt in Flüssen usw. In modernen Städten leiten Versorgungsunternehmen aufbereitetes Grund- oder Flusswasser über Rohrleitungen in die Haushalte. Oder weshalb bezahlen Sie Ihre Wasserrechnung? Sicherlich bezahlen Sie für das »verbrauchte« Wasser, aber auch dafür, dass Wasser mehr oder weniger konstant fließt, wenn Sie am Hahn drehen. Das Wasser steht in den Rohrleitungen unter Druck und wartet nur darauf, dass Sie den Hahn aufdrehen.

Im Grunde genommen funktioniert die Elektrizität ähnlich wie Wasser. Die überall vorhandenen Elektronen werden vom Elektrizitätswerk unter Druck über Leitungen in die Haushalte geliefert. Wie das Wasser befinden sich auch die Elektronen in den Leitungen und wartet nur darauf, dass Sie einen Stecker in die Wandsteckdose stecken. Anschließend fließt der Strom mehr oder weniger konstant. Sie verbinden eine Lampe mit der Steckdose, betätigen den Schalter, der Strom fließt und schon geht das Licht an. Sie zahlen für die Verlässlichkeit, den »Druck« der Elektronen und die verbrauchte Energie.

Der Druck der Elektronen in der Leitung wird *Spannung* genannt und in der Einheit *Volt* (V) angegeben (Abbildung 7.2).

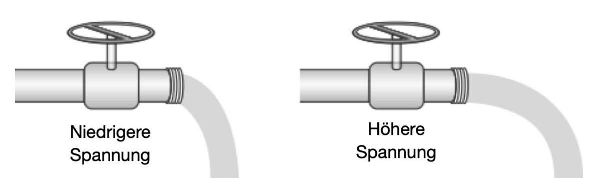


Abb. 7.2: Elektrische Spannung als Wasserdruck

Die Menge der Elektronen, die pro Zeiteinheit die Leitung durchlaufen, wird *Stromstärke* genannt und in *Ampere* (Abkürzung A, benannt nach dem französischen Physiker André-Marie Ampère, dennoch wird die Einheit im deutschen und englischen Sprachraum üblicherweise ohne Akzent geschrieben) angegeben (Abbildung 7.3).

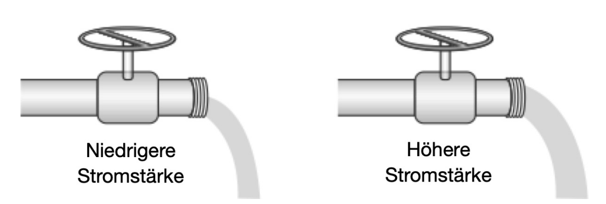


Abb. 7.3: Elektrische Stromstärke als Flussmenge des Wassers

Die Stromstärke und Spannung, die von einem bestimmten Gerät benötigt wird, damit es funktionieren kann, wird *Wattleistung* oder auch *elektrische Leistung* genannt und in *Watt* (W) angegeben. Die Beziehung zwischen den drei Größen lässt sich durch eine einfache Gleichung ausdrücken: V x A = W. Mit der Wattleistung werden wir uns später in diesem Kapitel noch sehr viel ausführlicher befassen.

Leitungen aller Art, seien sie nun aus Kupfer, Zinn, Gold oder Platin, bieten dem Fluss der Elektronen einen gewissen Widerstand, ähnlich wie dies auch für den Reibungswiderstand in Wasserleitungen gilt, der den Wasserfluss behindert. Der sich dem Elektronenfluss bietende elektrische *Widerstand* wird in *Ohm* (Ω) angegeben.

- Druck = Spannung (V)
- Flussmenge = Ampere (A)
- Arbeit/Leistung = Watt (W)
- Widerstand = Ohm (Ω)

Leitungen mit einem bestimmten Durchmesser können jeweils nur eine gewisse Menge Elektronen pro Zeiteinheit verkraften. Wenn zu viele Elektronen fließen sollen, dann schmilzt (bzw. platzt) die Leitung, ähnlich wie dies auch bei überlasteten Wasserleitungen der Fall ist. Eine bestimmte Leitung eignet sich nur für eine gewisse maximale Stromstärke, wie z.B. 20 Ampere. Wenn Sie 30 Ampere durch eine 20-Ampere-Leitung schicken, dann schmilzt die Leitung und die frei werdenden Elektronen suchen sich einen Weg, um das Spannungsgefälle auszugleichen. Und das kann ziemlich ungesund sein, wenn dieser Weg durch Ihren Körper hindurchführt!

Leistungsschutzschalter und Erdungsleitungen bieten einen gewissen Schutz davor. Ein Leistungsschutzschalter ist ein wärmeempfindlicher elektrischer Schalter, der für eine bestimmte Stromstärke ausgelegt ist. Wird der durch den Leistungsschutzschalter fließende Strom zu groß, erkennt der Schutzschalter das und unterbricht den Stromfluss, bevor die Schaltung überhitzt und zerstört wird. Sie können den Leistungsschutzschalter durch das Drücken eines Knopfes wieder einschalten, sodass der Strom wieder fließt. Eine *Erdungsleitung* (*Erdung*) sorgt für einen Weg des geringsten Widerstands für die Elektronen, sodass diese bei unbeabsichtigtem Stromfluss in die Erde abgeführt werden können.

Früher wurden in Netzteilen Sicherungen statt Leistungsschutzschaltern verwendet. Sicherungen sind kleine Bauteile, in denen sich ein Draht befindet, der nur eine bestimmte Stromstärke aushält. Ist der durch die Sicherung fließende Strom zu groß, schmilzt der Draht. Die Sicherung ist dann »durchgebrannt« und muss ersetzt werden. Der Einsatz von Leistungsschutzschaltern ist daher sehr viel sinnvoller. Auch wenn man heutzutage kaum noch Sicherungen verwendet, die durchbrennen können, findet man sie noch in vielen elektrischen Geräten, wie z.B. im Netzteil eines PCs, um es selbst intern zu schützen. Ist eine solche Sicherung erst einmal durchgebrannt, muss sie von einem Benutzer oder Techniker mit entsprechender Ausbildung und geeignetem Werkzeug ersetzt werden.

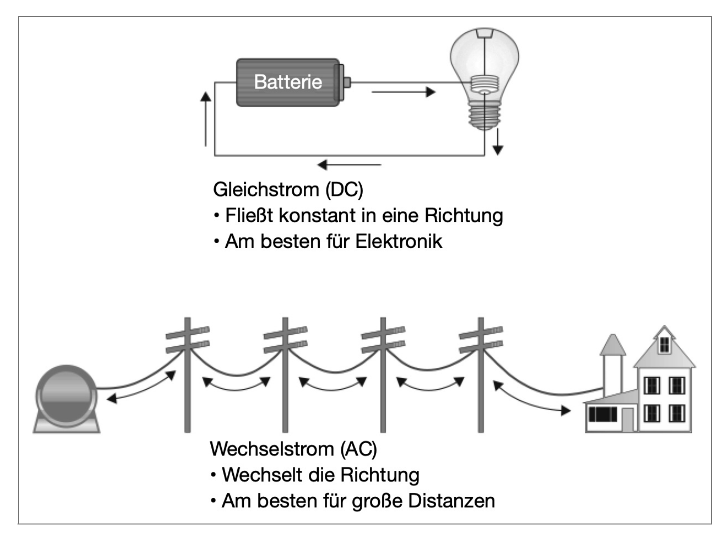


Abb. 7.4: Der unterschiedliche Fluss der Elektronen bei Gleich- und Wechselstrom

Wichtig

Steckdosen müssen geerdet sein, um sich für den Anschluss eines Rechners zu eignen!

Es gibt zwei Arten von Strom. Beim *Gleichstrom* (*DC – Direct Current*) fließen die Elektronen in einem geschlossenen Schaltkreis in einer Richtung, während die Elektronen beim Wechselstrom (AC – *Alternating Current*) im Schaltkreis abwechselnd in die eine oder andere Richtung fließen (siehe Abbildung 7.4). Die meisten elektronischen Geräte verwenden Gleichstrom, aber alle Energieversorgungsunternehmen liefern Wechselstrom, weil Wechselstrom über große Distanzen effizienter transportiert werden kann als Gleichstrom.

1001

7.2 Stromversorgung des Rechners

Der PC benötigt Gleichstrom, während die Energieunternehmen nur Wechselstrom liefern. Die Spannung muss also irgendwie gewandelt werden, damit der Rechner funktionieren kann. Das Netzteil in einem Computer wandelt die Wechselspannung in niedrige Gleichspannung um. Zunächst muss der PC daher ausreichend und gleichmäßig mit Wechselstrom versorgt werden. Dann muss das Netzteil die Wechselspannung in geeignete Gleichspannung mit passender Stromstärke für das Mainboard und die Peripheriegeräte umwandeln. Und schließlich gilt es, die Abwärme als Nebenprodukt der Elektrizität zu handhaben. Befassen wir uns also eingehender mit der Stromversorgung des PCs.

7.2.1 Wechselspannungsversorgung

Alle PC-Netzteile müssen mit einer Steckdose verbunden und mit gleichmäßiger Spannung versorgt werden sowie einen gewissen Schutz bei gelegentlichen Schwankungen der Versorgungsspannung bieten. Das Netzteil wird über ein Netzkabel mit *Kaltgerätestecker* (*IEC-320-Anschluss*) und das Stromkabel mit der Wandsteckdose verbunden. Die Versorgungsspannung liegt in den meisten europäischen Ländern zwischen 220 und 240 Volt (Wechselspannung), während sie vorwiegend in den USA zwischen 110 und 120 Volt liegt. Manchmal verfügen Netzteile über einen kleinen Schalter an der Rückseite, über den sie an die jeweilige Versorgungsspannung angepasst werden können. Netzteile, die man nicht manuell umschalten muss, werden als auto-switching bezeichnet. Abbildung 7.5 zeigt die Rückseite eines Netzteils. Beachten Sie die drei Elemente, bei denen es sich (von oben nach unten) um den Netzschalter, den 115/230-Spannungswahlschalter und die Buchse für den Kaltgerätestecker handelt.



Abb. 7.5: Rückseite eines Netzteils mit typischen Schaltern und Stromanschluss

Vorsicht

Wenn der Schalter zur Anpassung an die Netzspannung an der Rückseite eines Netzteils versehentlich falsch eingestellt wird, können die Folgen für den Rechner fatal sein! Wenn die Netzspannung ca. 115 Volt beträgt (wie z.B. in den USA) und Sie den Schalter (bei abgeschaltetem Rechner) auf 230 Volt einstellen, dann versucht der Rechner wahrscheinlich zwar zu booten, dürfte dabei aber nicht weit kommen. Damit können Sie zwar Kollegen ärgern, echte Schäden stehen aber kaum zu befürchten. Wenn die Netzspannung allerdings (wie in Deutschland und den meisten europäischen Ländern) ca. 230 Volt beträgt und Sie den Rechner mit der Schalterstellung 115 Volt starten, dann dürfte das Netzteil schnell in Rauch aufgehen. Achten Sie also auf diesen Schalter, sofern er vorhanden ist!

Bevor Sie überhaupt Geräte mit Wechselspannung über die Steckdose mit Strom versorgen, sollten Sie als Erstes deren Spannung mit einem *Multimeter* oder einem anderen Gerät prüfen, das sich speziell für diesen Zweck eignet. Versäumen Sie die Prüfung der Spannungsversorgung, kann dies zum Funktionsausfall oder zur Beschädigung von Geräten, aber auch zu für Menschen gefährlichen Stromschlägen führen. Der IEC-320-Stecker besitzt drei Leitungen: den Außenleiter (umgangssprachlich »Phase«), den Neutralleiter (»Null«) und den Schutzleiter (»Erde«). Diese Namen beschreiben die Funktion der Leitungen, die hinter der Abdeckung damit verbunden sind. Der Außenleiter ist stromführend, ähnlich wie ein Rohr, das Wasser bereitstellt. Am Neutralleiter liegt normalerweise keine Spannung an, er verhält sich mehr wie ein Wasserabfluss, wodurch der Kreislauf vervollständigt wird, indem Elektronen an die lokale Stromquelle zurückgeleitet werden, normalerweise in einen Schaltkasten. Der Neutralleiter ermöglicht es beispielsweise, dass überschüssige Elektronen sicher zur Erde zurückgelangen, etwa bei einem Kurzschluss.

Bei der Spannungsversorgung prüfen Sie drei Dinge: die Versorgung des stromführenden Leiters mit etwa 230 V, die korrekte Erdung des neutralen Leiters (0 V) und die korrekte Erdung des Schutzleiters (wiederum 0 V). Abbildung 7.6 zeigt die an einer Steckdose anliegenden Spannungen.

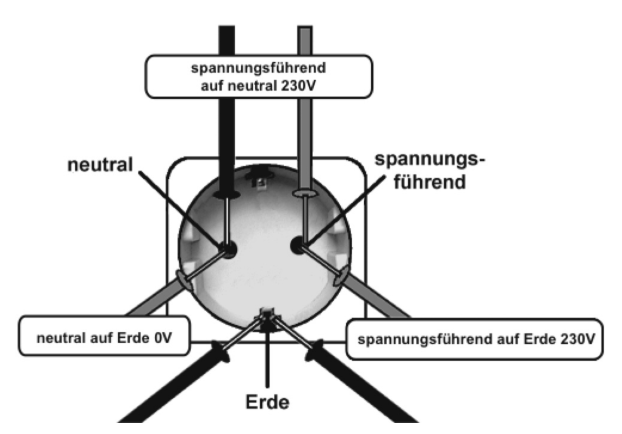


Abb. 7.6: Spannungspegel einer Steckdose

Mit einem *Multimeter* (auch DMM – Digitalmultimeter – oder Volt-Ohm-Meter genannt) können Sie eine Reihe verschiedener Eigenschaften des elektrischen Stroms messen. Ein Multimeter verfügt über zwei Prüfspitzen, eine analoge oder digitale Anzeige und einen Wählschalter, über den Sie die Art der durchzuführenden Messung einstellen. Abbildung 7.7 zeigt die verschiedenen Bestandteile eines Multimeters.

Beachten Sie, dass bei einigen Multimetern Symbole anstelle von Beschriftungen zur Beschreibung der Einstellungen für Gleich- und Wechselspannung verwendet werden. Das »V« mit der durchgehenden Linie oben und der gestrichelten unten in Abbildung 7.8 symbolisiert so z.B. Gleichspannung (DC). Das Symbol »V~« steht für Wechselspannung (AC).



Abb. 7.7: Das alte aber zuverlässige Multimeter des Autors

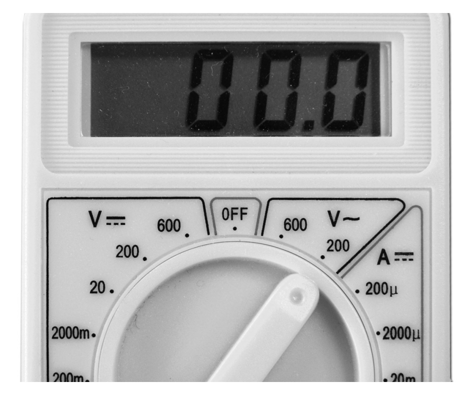


Abb. 7.8: Multimeter, bei dem Gleich- und Wechselspannung durch Symbole dargestellt werden

Die meisten Multimeter ermöglichen mindestens vier verschiedene elektrische Messungen: Durchgangsprüfung, Widerstand, Wechselspannung (VAC) und Gleichspannung (VDC). Bei der *Durchgangsprüfung* wird getestet, ob Elektronen von einem Ende einer Leitung zum anderen fließen können. Wenn das der Fall ist, dann leitet ein Draht, andernfalls nicht. Diese Einstellung können Sie dazu verwenden, um Kabelbrüche oder defekte Sicherungen zu erkennen. Falls Ihr Multimeter keine Durchgangsprüfung bietet (was bei vielen billigeren Multimetern der Fall ist), können Sie stattdessen auch den Leitungswiderstand messen. Eine defekte Leitung oder Sicherung zeigt einen unendlichen Widerstand, während der Widerstand intakter Leitungen oder Sicherungen nahe null liegt. Beim Testen von Wechsel- und Gleichspannungen überprüfen Sie, ob die gemessenen Spannungen den jeweiligen Sollwerten entsprechen.

Tipp: Wechselstrom mit einem Multimeter prüfen

Als kompetenter Techniker sollten Sie wissen, wie ein Multimeter eingesetzt wird, und falls Sie noch nie eines benutzt haben, besorgen Sie sich so ein Gerät und führen Sie die folgende Übung durch! Ihr Chef hat Sie beauftragt, in der neuen Zweigstelle die vorhandenen Steckdosen zu überprüfen. Achtung: Berühren Sie keine Teile aus Metall, weder an der Steckdose noch an den Prüfspitzen des Multimeters!

Führen Sie zunächst zur Messung von Wechselspannungen mit dem Multimeter die nachfolgenden Schritte durch:

1. Stellen Sie den Wählschalter auf Wechselspannung (AC, normalerweise rot markiert) ein. Falls es mehrere Auswahlmöglichkeiten geben sollte, stellen Sie einen Skalenbereich oberhalb von 230 Volt ein. Sollte das Multimeter automatisch einen eigenen Bereich auswählen, ist keine weitere Einstellung außer AC erforderlich.
2. Verbinden Sie das schwarze Messkabel mit der Steckverbindung am Multimeter mit dem Minuszeichen (–). Diesen Schritt können Sie übergehen, falls die schwarze Prüfspitze fest angeschlossen ist.
3. Verbinden Sie das rote Kabel mit der Steckverbindung des Multimeters mit dem Pluszeichen (+) und der Kennzeichnung V. Diesen Schritt können Sie übergehen, falls die rote Prüfspitze fest angeschlossen ist.

Wenn Sie das Multimeter für die Messung von Wechselspannung eingestellt haben, dann können Sie die verschiedenen Kontakte an einem Wechselspannungsanschluss prüfen. Berühren Sie aber nicht das Metall der Prüfspitzen, wenn Sie diese in die Steckdose einführen! Führen Sie die folgenden Schritte aus:

1. Legen Sie eine Prüfspitze am spannungsführenden und die andere am neutralen Leiter an. Sie müssten daraufhin ca. 230 Volt Wechselspannung ablesen können.
2. Legen Sie eine Prüfspitze am spannungsführenden Leiter und die andere an Erde an. Sie müssten daraufhin ca. 230 Volt Wechselspannung ablesen können.
3. Legen Sie eine Prüfspitze am neutralen Leiter und die andere an Erde an. Sie müssten daraufhin ca. 0 Volt Wechselspannung ablesen können.

Falls Sie andere Messwerte erhalten, sollten Sie einen Elektriker rufen!

Spezielle Geräte zur Messung von Wechselspannung

Es gibt eine ganze Reihe von Geräten, mit denen nur Wechselspannung bzw. Steckdosen überprüft werden können (Abbildung 7.9). Stecken Sie das Gerät einfach in die Steckdose, um die Spannungen zu überprüfen. Testen Sie alle vom Computersystem verwendeten Steckdosen: Netzteil, externe Geräte und Monitor. Die speziellen Geräte sind zwar praktisch, aber lange nicht so genau wie Multimeter. Oft werden gegebenenfalls vorhandene Fehler über LEDs angezeigt.



Abb. 7.9: Spannungsprüfer

Steckernetzteile

Viele Geräte im Computerbereich benutzen Steckernetzteile und keine internen Netzteile. Aber auch wenn sich das Steckernetzteil außerhalb des Geräts befindet, wandelt es ebenfalls Wechselstrom in Gleichstrom um. Anders als Rechnernetzteile lassen sich Steckernetzteile aber nicht beliebig untereinander austauschen, selbst wenn die Stecker am Ende der von den Steckernetzteilen wegführenden Kabel identisch sind. Anders ausgedrückt: Wenn das Steckernetzteil des Laptops eines Bekannten in Ihren Laptop »passt«, heißt das noch lange nicht, dass es auch funktioniert.

Bevor Sie ein Steckernetzteil oder ein anderes externes Netzteil mit einem Gerät verbinden, müssen Sie drei technische Eigenschaften prüfen. Dabei handelt es sich um die abgegebene Spannung, die Stromstärke und die Polarität. Bei zu niedriger Spannung oder Stromstärke wird das Gerät nicht funktionieren. Ist die Polarität vertauscht, wird es ebenfalls nicht funktionieren, wie bei einer Taschenlampe, bei der Sie eine der Batterien verkehrt herum einsetzen. Ist die Stromstärke oder insbesondere die Spannung zu hoch, kann Ihr Gerät ziemlich schnell durchschmoren. Überprüfen Sie also immer Spannung, Stromstärke und Polarität, bevor Sie ein Steckernetzteil mit einem Gerät verbinden.

1002

Erdung

Der Schutz des Computers beginnt mit einer korrekten Erdung. Die Erdung dient als eine Art Notausgang für überschüssigen Strom, wenn es in einem Gerät zu einem Kurzschluss oder einer Fehlfunktion kommt. Sie dürfen nicht davon ausgehen, dass alle Steckdosen auch tatsächlich richtig geerdet sind, vor allem nicht in älteren Gebäuden. Überprüfen Sie das mit einem Multimeter.

Schutz des PCs vor Spannungsschwankungen

Wenn alle Energieversorgungsunternehmen eine gleichmäßige Stromversorgung ohne Spannungsabfälle und -spitzen liefern würden, dann wären die nächsten beiden Abschnitte dieses Kapitels überflüssig. Egal, wie sauber die Wechselstromversorgung für ein Multimeter jedoch erscheinen mag, ist es leider so, dass die vom Stromversorgungsunternehmen kommende Spannung gelegentlich deutliche Schwankungen in beide Richtungen aufweist. Diese *Spannungsabfälle* und *Spannungsspitzen* wirken sich normalerweise nicht negativ auf Lampen oder Kühlschränke aus, können aber dafür sorgen, dass Ihr PC abstürzt oder nicht mehr läuft, und sie können einen PC oder ein Peripheriegerät sogar zerstören. Es gibt zwei Geräte, die sich um Spannungsabfälle und -spitzen kümmern: Überspannungsschutz und unterbrechungsfreie Stromversorgungen.

Überspannungsschutz Spannungsspitzen sind sehr viel gefährlicher als Spannungsabfälle. Selbst ein großer Spannungsabfall schaltet Ihren PC nur aus oder sorgt für einen Absturz und anschließenden Neustart. Eine Spannungsspitze hingegen kann Ihren Computer beschädigen, und eine große Spannungsspitze kann Komponenten zerstören. Weil Spannungsspitzen so gefährlich sind, sollte jeder PC mit einem *Überspannungsschutz* ausgerüstet werden, der überhöhte Spannungen unterdrückt und damit den PC schützt. Gute Netzteile sorgen bereits für einen recht guten Überspannungsschutz und kommen mit den kleineren und relativ häufigen Spannungsspitzen zurecht. Dadurch kann das Netzteil jedoch beschädigt werden und irgendwann ausfallen. Um Ihr Netzteil und das System zuverlässig vor Überspannungen zu schützen, sollte zwischen Netzteil und Steckdose ein Überspannungsschutz geschaltet werden (Abbildung 7.10).

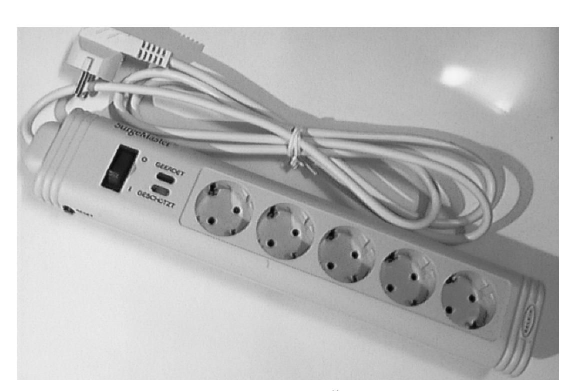


Abb. 7.10: Steckdosenleiste mit Überspannungsschutz

Viele Leute geben zwar viel Geld für ihre Rechner aus, sparen aber beim Überspannungsschutz. Lassen Sie sich im Fachhandel beraten, wie Sie Ihre wertvollen PC-Komponenten am besten vor Überspannungen schützen können. Prüfen Sie, für wie viel Joule die Überspannungseinrichtung ausgelegt ist. *Joule* ist eine Maßeinheit für die elektrische Energie und beschreibt die zulässige Menge, die ein Überspannungsschutz bis zum Totalausfall vertragen kann. Empfohlen wird oftmals eine Mindestbelastbarkeit von 2.000 Joule, wobei der Schutz umso größer ist, je mehr Joule verkraftet werden! Für meinen Überspannungsschutz wird eine Belastbarkeit von 3.500 Joule angegeben.

Und da wir gerade beim Schutz des Systems sind, vergessen Sie nicht, dass auch bei Telefonleitungen und Kabelverbindungen Spannungsspitzen auftreten können. Wenn Sie ein Modem, DSL oder ein Kabelmodem einsetzen, sollten Sie einen Überspannungsschutz benutzen, der diese Anschlussarten schützt. Viele Hersteller kombinieren daher den Überspannungsschutz für die Stromleitungen mit dem für Telefonleitungen (Abbildung 7.11).

Vorsicht

Auch der beste Überspannungsschutz ist den enormen Ladungen eines Blitzeinschlags nicht immer gewachsen. Wenn ein elektrisches System mit der Steckdose verbunden ist und von einem derartigen Schlag getroffen wird, dann können Sie sich vermutlich von ihm verabschieden. Während eines Unwetters empfiehlt es sich daher, elektronische Geräte möglichst von der Steckdose zu trennen.



Abb. 7.11: Überspannungsschutz für Telefonleitungen

Kein Überspannungsschutz hält ewig. Achten Sie darauf, dass es am Überspannungsschutz einen Test-/Reset-Schalter gibt, der Ihnen mitteilt, ob das Gerät womöglich nur noch als Verlängerungskabel arbeitet – wie die Profis es gerne ausdrücken. Wenn Ihr System beschädigt wird, obwohl Sie einen Überspannungsschutz haben, wenden Sie sich an den Hersteller. Viele Unternehmen bieten Versicherungen und Entschädigungen an, wenn Ihr System aufgrund von Spannungsspitzen ausfällt, die Sie aber nur erhalten, wenn Sie sich streng an die Richtlinien halten.

Hinweis

Beim Überspannungsschutz zählt nicht nur die Belastbarkeit in Joule. Oft ist auch eine Begrenzungsspannung angeben, bei der eine Spannungsspitze kurzzeitig auf eine niedrigere Spannung heruntergeregelt wird. Gute Geräte schaffen es, Spannungen von 600 Volt für 50 Mikrosekunden auf 180 Volt oder weniger zu begrenzen (entweder auf der spannungsführenden oder auf der neutralen Leitung).

Wenn Sie einen wirklich guten Überspannungsschutz benötigen, müssen Sie für eine *Spannungsstabilisierung* (*Power Conditioning*) sorgen. Ihre Stromleitungen nehmen alle möglichen seltsamen Signale auf, die dort nichts zu suchen haben, wie beispielsweise elektromagnetische Störungen (EMI – Elektromagnetische Interferenzen) oder Funkstörungen (RFI – Radio Frequency Interference). Größtenteils ist dieses Leitungsrauschen so minimal, dass man sich nicht darum kümmern muss, aber bestimmte Ereignisse (z.B. Blitze) erzeugen genügend Leitungsrauschen, um unangenehm für Ihren PC zu werden (Tastaturabstürze, zerstörte Daten). Jeder bessere Überspannungsschutz verfügt über eine Spannungsstabilisierung, die (in Grenzen) auch elektromagnetische Störungen oder Funkfrequenzstörungen herausfiltern kann.

USV (Unterbrechungsfreie Stromversorgung) Eine *USV* (*Unterbrechungsfreie Stromversorgung*) bzw. *UPS* (*Uninterruptible Power Supply*) schützt Ihren Rechner (und, was noch wichtiger ist, Ihre Daten) im

Falle von Spannungsabfällen oder Ausfällen der Stromversorgung. Abbildung 7.12 zeigt eine typische USV. Eine USV besteht im Wesentlichen aus einer starken Batterie, die unabhängig vom Zustand der über die Steckdose gelieferten Netzspannung immer eine konstante Wechselspannung an den PC abgibt.



Abb. 7.12: Unterbrechungsfreie Stromversorgung

In den Datenblättern aller unterbrechungsfreien Stromversorgungen finden Sie Angaben in Watt (die tatsächliche Menge an Energie, die sie bei einem Stromausfall zur Verfügung stellen) und Volt-Ampere (VA). Bei der letzteren Angabe handelt es sich um die Energie, die eine USV liefern kann, wenn die Geräte ihren Strom komplett über sie beziehen. Ihre USV sorgt für den perfekten Wechselstrom mit einer schön gleichmäßigen Frequenz von 50 Hertz (Hz). Netzteile, Bildschirme und andere Geräte verwenden jedoch im zeitlichen Mittel nicht die konstante Energiemenge, die die USV bereitstellt, sodass sie ineffizient arbeitet. Wenn Ihre Geräte zu jedem Zeitpunkt die gesamte von der USV angebotene Energie verbrauchen würden, wäre VA gleich Watt.

Wenn die USV-Hersteller im Voraus wüssten, welche Geräte Sie an ihre USVs anschließen wollen, könnten sie Ihnen die genaue Wattzahl angeben, aber unterschiedliche Geräte arbeiten unterschiedlich effizient, wodurch die USV-Hersteller angeben müssen, was USVs anbieten können (in VA), und nicht das, was Ihre Geräte verbrauchen (in Watt). Beim angegebenen Watt-Wert handelt es sich um eine Schätzung, die nie so hoch wie die VA-Angabe ist.

Wichtig

Für die CompTIA A+-Prüfung 220-1002 sollten Ihnen Überspannungsschutz und unterbrechungsfreie Stromversorgung geläufig sein.

Weil sich die Effizienz aller an die USV angeschlossenen Geräte nie genau messen lässt, sollten Sie sich an die Watt-Angabe halten. Addieren Sie die Gesamtleistung der einzelnen Komponente im PC und kaufen Sie eine USV mit höherer Leistung. Sie werden eine Menge Zeit aufwenden und ein wenig Denkarbeit leisten müssen, um genau zu ermitteln, wie viel Leistung Ihr Computer, Bildschirm, die Laufwerke usw. benötigen, um die richtige USV für Ihr System zu kaufen. Aber damit sind Sie noch nicht fertig! Sie wissen, dass die USV eine Batterie mit begrenzter Leistung ist, deshalb müssen Sie herausfinden, wie lange die USV Strom bereitstellen soll, wenn bei Ihnen der Strom ausfällt.

Hinweis

Es gibt zwei USV-Hauptvarianten. Bei der Online-USV werden die Geräte andauernd über die Batterie der USV mit Strom versorgt, während sie bei der Standby-USV nur dann von der USV versorgt werden, wenn die Spannung unter einen bestimmten Mindestwert sinkt. Eine weitere Variante wird Line-Interactive-USV genannt. Sie ähnelt zwar der Standby-USV, besitzt aber spezielle Schaltkreise, die moderate Spannungsschwankungen ausgleichen können, ohne dass gleich auf die Batterieversorgung umgeschaltet werden müsste.

Schneller und besser können Sie feststellen, welche USV Sie brauchen, wenn Sie eine der Websites der großen Hersteller von Überspannungsschutz oder USVs besuchen und deren praktische Leistungsrechner benutzen. Mein persönlicher Favorit findet sich auf der Website von APC/Schneider Electric (ehemals American Power Conversion Corporation) unter `www.apc.com`. (Geben Sie `UPS selector` in das Suchfeld ein.) APC stellt ausgezeichnete Überspannungsschutzgeräte und USVs her. Der Online-Rechner des Unternehmens zeigt Ihnen die tatsächliche Wattzahl an, die sie benötigen. Dort erfahren Sie gleichzeitig auch mehr über die aktuellen Fortschritte in diesem Bereich.

Tipp: Kauf einer USV

Wenn Sie für sich selbst oder einen Kunden eine USV erwerben möchten, können Sie sich am besten einen Eindruck von den im Marketing verwendeten Begriffen verschaffen, indem Sie Ihren örtlichen Computerhändler besuchen. Sie brauchen einen Vorwand, um mal wieder zum Händler zu gehen? Hier ist einer.

1. Sehen Sie sich beim Händler oder, falls es keine geeigneten Geschäfte in Ihrer Nähe gibt, im Internet an, welche Geräte verfügbar sind.
2. Beantworten Sie die folgende Frage: Wie kann man feststellen, ob es sich bei einem Gerät um eine Online- oder um eine Standby-USV handelt?

Alle USVs beinhalten Überspannungsschutz und Spannungsstabilisierung, achten Sie daher auf die Joule-Angabe und die Begrenzungsspannung. Informieren Sie sich auch über die Kosten für Austauschbatterien, die teilweise ziemlich teuer sein können. Außerdem sollten Sie möglichst eine intelligente USV mit USB- oder Ethernet-Anschluss (RJ-45) kaufen. Diesen praktischen USVs liegen Überwachungs- und Wartungsprogramme bei (Abbildung 7.13), die Auskunft über den Systemstatus und den verfügbaren Batteriestrom geben können, wichtige Ereignisse protokollieren und weitere praktische Funktionen bereitstellen.

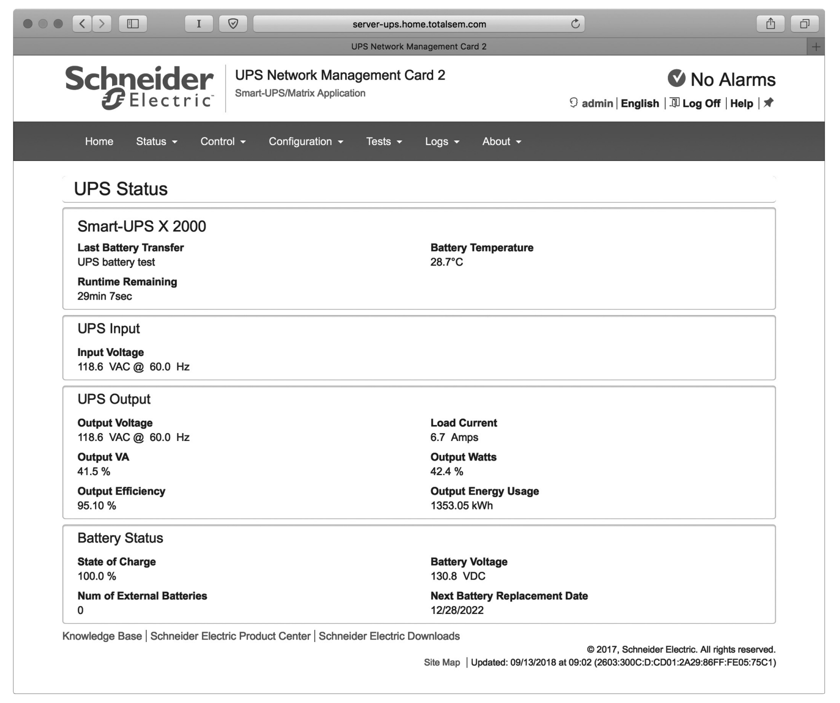


Abb. 7.13: Anwendung zur Steuerung und Überwachung einer USV

In Tabelle 7.1 finden Sie Merkmale sehr einfacher und besserer USV-Modelle.

Marke	Modell	Steckdosen	Leistung	Typ
APC	BE425M	3	3 Min. @ 200 W; 10 Min. @ 100 W	Standby
APC	Pro BR 1000MS	4	4 Min. @ 600 W; 64 Min. @ 100 W	Standby
CyberPower	CPS1500AVR	6	6 Min. @ 950 W; 18 Min. @ 475 W	Line-interactive

Tabelle 7.1: Typische USVs

1001

7.2.2 Versorgung mit Gleichspannung

Wenn Sie sich davon überzeugt haben, dass die Wechselspannungsversorgung in Ordnung ist, dann kommt das Netzteil an die Reihe, das die hohe Wechselspannung von 230 Volt für die empfindlichen internen Rechnerkomponenten in verschieden hohe Gleichspannungen umwandelt (insbesondere 12,0, 5,0 und 3,3 Volt). Netzteile gibt es zwar in den unterschiedlichsten Formen und Größen, bei Weitem am gebräuchlichsten sind aber Desktop-Netzteile mit den Standardabmessungen 150x140x86 mm (Abbildung 7.14).



Abb. 7.14: Desktop-Netzteil

Die 12,0-Volt-Spannung wird im Rechner für den Antrieb der Motoren von Festplatten oder CD/DVD-Laufwerken verwendet, während die 5,0- und 3,3-Volt-Spannungen für die Schaltkreise auf den verschiedenen Platinen genutzt werden. Die Hersteller können die verschiedenen Spannungen allerdings beliebig einsetzen und damit auch von der ansonsten üblichen Verwendung abweichen. Netzteile sind mit Standardanschlüssen für das Mainboard und die internen Komponenten ausgestattet.

Stromversorgung des Mainboards

Moderne Mainboards verwenden einen 20- oder 24-poligen *P1-Stromanschluss*. Einige Mainboards benötigen möglicherweise spezielle 4-, 6- oder 8-polige Stecker für eine zusätzliche Stromversorgung

(Abbildung 7.15). Ich komme später in diesem Kapitel bei der Beschreibung der Formfaktor-Standards noch auf diese Stecker zurück.

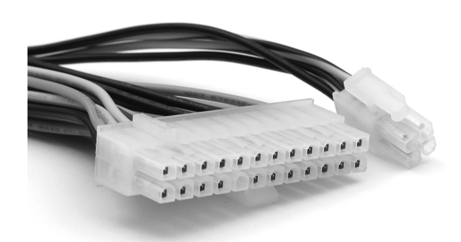


Abb. 7.15: Stecker für die Stromversorgung des Mainboards

Anschluss der Peripheriegeräte: Molex, Mini-Molex und SATA

Im PC benötigen viele Komponenten Strom, wie z.B. Festplatten, SSD-Laufwerke, optische Laufwerke und Lüfter. Das typische PC-Netzteil verfügt über mindestens drei verschiedene Steckervarianten für den Anschluss von Peripheriegeräten: Molex, Mini(-Molex) und SATA. (Hochwertige Grafikkarten verfügen über eigene Anschlüsse; mehr dazu später in diesem Kapitel.)

Molex-Anschlüsse Der Molex-Stecker wird für Geräte verwendet, die Spannungen von 12 und 5 Volt benötigen (Abbildung 7.16). Der Molex-Stecker hat zwei Abschrägungen, die eine korrekte Ausrichtung des Steckers erleichtern. Beim Anschluss des Molex-Steckers muss dieser mit kräftigem Druck in die Buchse gedrückt werden und mit roher Gewalt lassen sich die Stecker auch verkehrt herum einsetzen. Da das nicht gut wäre, sollten Sie *immer* erst einmal prüfen, ob der Stecker richtig herum eingesetzt wird!

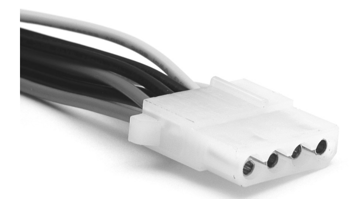


Abb. 7.16: Molex-Stecker

Mini-Anschlüsse Manche Netzteile verfügen über einen zweiten Anschlusstyp, der *Mini-(Molex-)Anschluss* genannt wird (Abbildung 7.17), der Peripheriegeräte ebenfalls mit 5 und 12 Volt Spannung versorgt. Die Hersteller von Diskettenlaufwerken hatten den Mini-Stecker standardmäßig für 3,5-Zoll-Laufwerke übernommen, aber gelegentlich begegnet man immer noch Geräten, die diesen Anschluss verwenden.

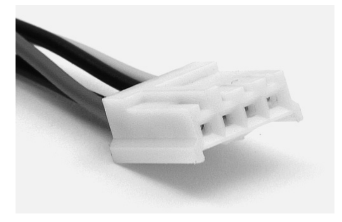


Abb. 7.17: Mini-(Molex-)Stecker

Tipp: Gleichspannung überprüfen

Ein gängiges Verfahren zur Fehlersuche ist das Überprüfen der vom Netzteil gelieferten Gleichspannung. Auch wenn die Wechselspannungsversorgung in Ordnung ist, kann es vorkommen, dass ein defektes Netzteil nicht die von Mainboard und Peripheriegeräten benötigte Gleichspannung bereitstellt. Probieren Sie diese Vorgehensweise am besten selbst aus. Nehmen Sie Ihr Multimeter zur Hand und führen Sie die folgenden Schritte an einem eingeschalteten PC durch, dessen Seitenwand entfernt ist. Beachten Sie, dass der P1-Stromanschluss am Mainboard angeschlossen sein muss und dass das System läuft. (Es ist natürlich nicht notwendig, dass Windows oder Linux gestartet wurde.)

1. Stellen Sie bei Ihrem Multimeter den Messbereich für Gleichspannung (DC) auf etwa 20 Volt ein (sofern das erforderlich ist). Vergewissern Sie sich, dass die Prüfspitzen korrekt angeschlossen sind: die rote am Plus-Anschluss und die schwarze am Masseanschluss (Ground). Bei der Messung von Gleichspannungen muss die Polarität beachtet werden. Die rote Prüfspitze wird an spannungsführende Leitungen jeglicher Farbe angeschlossen, die schwarze wird *immer* mit Masse verbunden.
2. Schließen Sie die rote Prüfspitze an eine mit einer roten Leitung verbundene Molex-Stecker-Buchse und die schwarze Prüfspitze an eine der beiden mit einer schwarzen Leitung verbundenen Molex-Stecker-Buchsen an. Sie sollten ungefähr 5 Volt messen. Was wird Ihnen angezeigt?
3. Schließen Sie nun die rote Prüfspitze an die mit einer gelben Leitung verbundene Buchse an. Welche Spannung messen Sie jetzt?
4. Das Überprüfen des P1-Stromanaschlusses ist etwas umständlicher. Führen Sie die rote und die schwarze Prüfspitze so von oben in den P1-Stecker ein, dass sie an den Leitungen entlang nach unten gleitet, bis sie schließlich Kontakt bekommt. Belassen Sie die schwarze Prüfspitze in einem der mit einer schwarzen Leitung verbundenen Masseanschlüsse und messen Sie mit der roten Prüfspitze der Reihe nach alle Anschlüsse mit farbigen Leitungen durch. Welche Spannungen messen Sie?

Vorsicht

Wie bei allen Stromanschlüssen führt auch beim Mini-Stecker die falsche Polung sehr wahrscheinlich zur Beschädigung der entsprechenden Komponente. Überzeugen Sie sich also besser zweimal, ob der Stecker richtig orientiert ist, bevor Sie ihn anschließen!

SATA-Stromanschlüsse SATA-Laufwerke (SATA) benötigen einen speziellen 15-poligen SATA-Stromstecker (Abbildung 7.18). Durch die zusätzlichen Pins unterstützen sie die Hot-Swapping-Funktion von SATA-Laufwerken und Geräte, die mit Spannungen von 3,3, 5,0 und/oder 12,0 Volt arbeiten. Die 3,3-Volt-Anschlüsse werden derzeit von keinem SATA-Laufwerk genutzt und sind für zukünftige Anwendungen reserviert. Alle drei SATA-Generationen verwenden den gleichen Stromanschluss. SATA-Stromstecker sind L-förmig, wodurch es fast unmöglich ist, sie falsch an SATA-Laufwerken anzuschließen. Andere Geräte verwenden den SATA-Stromstecker bislang nicht. Weitere Informationen über SATA-Laufwerke finden Sie in Kapitel 8, *Festplattentechnologien*.



Abb. 7.18: SATA-Stromstecker

Splitter und Adapter Manchmal gibt es möglicherweise nicht genug Stromstecker für alle Geräte im PC. Für solche Fälle gibt es *Splitter* (*Y-Kabel*), die für zusätzliche Anschlüsse sorgen (Abbildung 7.19). Möglicherweise brauchen Sie auch einen SATA-Stecker, haben aber nur noch einen Molex-Stecker

frei. Da die Spannungen der Leitungen bei beiden Varianten gleich sind, lässt sich dieses Problem leicht mit einfachen Adaptern beheben.



Abb. 7.19: Molex-Y-Kabel (Splitter)

ATX

Die Original-ATX-Netzteile besaßen zwei charakteristische physische Merkmale: den Mainboard-Stromstecker und *Softpower*. Der Strom für das Mainboard kam aus einem einzigen Kabel mit einem 20-poligen P1-Mainboard-Stromstecker. ATX-Netzteile verfügten außerdem über mindestens zwei weitere Kabel, an denen sich jeweils minimal zwei Molex- oder Mini-Molex-Stecker für die Stromversorgung von Peripheriegeräten befanden.

Wenn ATX-Systeme an die Steckdose angeschlossen sind, versorgen sie das Mainboard mit 5 Volt. Sie sind immer eingeschaltet, auch wenn der Rechner ausgeschaltet ist. Der Netzschalter, den Sie zum Einschalten des Rechners betätigen, ist kein echter Netzschalter, wie der Lichtschalter im Schlafzimmer. Der Netzschalter an einem ATX-System teilt dem Computer lediglich mit, dass er gedrückt wurde. Das BIOS oder das Betriebssystem übernimmt dann und sorgt dafür, dass der PC ein- oder ausgeschaltet wird. Dies wird auch *Softpower* genannt.

Die Verwendung von Softpower statt eines physischen Schalters hat mehrere wichtige Vorteile. Softpower verhindert, dass ein Benutzer ein System komplett ausschaltet, bevor das Betriebssystem heruntergefahren ist. Durch sie kann der PC Energiesparmodi nutzen, die das System in den Ruhezustand versetzen und es wieder aktivieren, wenn der Benutzer eine Taste drückt, die Maus bewegt oder eine E-Mail erhält (oder sonstiger Netzwerkverkehr stattfindet). Mehr über den Ruhezustand erfahren Sie in Kapitel 23, *Tragbare Computer*.

Die wichtigsten Einstellungen der Softpower-Funktion bei ATX-Systemen finden Sie im CMOS-Setup. Rufen Sie das CMOS-Setup auf und suchen Sie nach dem Bereich ENERGIEVERWALTUNG (Power Management). Abbildung 7.20 zeigt die POWER ON FUNCTION. Sie bestimmt die Arbeitsweise des Netzschalters. Sie können festlegen, dass der Rechner über diesen Schalter ausgeschaltet wird, oder Sie können ihn auf die übliche *Ausschaltverzögerung* von vier Sekunden setzen.

```
              Phoenix - Award BIOS CMOS Setup Utility
                      Power Management Setup

  ACPI Suspend Type            S3 (Suspend-To-RAM)    Item Help
  - USB Resume from S3         Enabled
  Power Button Function        Delay 4 Sec            Menu Level   ►
  Wake by PME# of PCI          Disabled
  Wakeup by Ring               Disabled
  Wakeup by OnChip LAN         Enabled
  Wakeup by Alarm              Disabled
x - Day of Month Alarm          0
x - Time (hh:mm:ss) Alarm      0 : 0 : 0
  AMD K8 Cool'n'Quite controlAuto
  Power On Function            Button Only
x - KB Power On Password       Enter
x - Hot Key Power On           Ctrl-F1
  Restore on AC Power Loss     Power Off

▲▼►◄:Move  Enter:Select    +/-/PU/PD:Value  F10:Save   ESC:Exit  F1:General Help
  F5:Previous Values         F6:Fail-Safe Defaults     F7:Optimized Defaults
```

Abb. 7.20: Softpower-Einstellungen im CMOS

Mehr als ein Jahrzehnt lang erledigte ATX die Aufgabe der Stromversorgung tadellos, aber mit der Zeit benötigten immer leistungsfähigere CPUs, Mehrkern-CPUs, Grafikkarten und andere Komponenten mehr und mehr Energie, die das ursprüngliche ATX-Netzteil nicht mehr liefern konnte. Deshalb wurde die Stromversorgung im ATX-Standard mehrfach überarbeitet und mit ATX12V 1.3, EPS12V, mehreren Spannungsschienen, ATX12V 2.0, anderen Formfaktoren und Active PFC weiterentwickelt.

ATX12V 1.3 Die erste weitverbreitete Aktualisierung des ATX-Standards, *ATX12V 1.3*, wurde 2003 veröffentlicht. Sie brachte einen 4-poligen Mainboard-Stromstecker mit sich, der inoffiziell aber allgemein als P4 bezeichnet wird und über den zur Unterstützung des 20-poligen P1-Mainboard-Steckers zusätzlich 12-Volt-Spannung bereitgestellt wird. Alle Netzteile mit einem P4-Stecker werden als ATX12V-Netzteil bezeichnet. Der Begriff »ATX« wurde aus dem ATX-Stromstandard entfernt, genau genommen gibt es also keine ATX-Netzteile. Alle Netzteile – vorausgesetzt, sie haben einen P4-Stecker – entsprechen ATX12V oder einem der neueren Standards.

Wichtig

SATA sieht auch einen Slimline-Anschluss mit sechs und einen Mikro-Anschluss mit neun Kontakten für die Stromversorgung vor.

ATX12V 1.3 führte außerdem einen zusätzlichen 6-poligen Stecker ein, der gemeinhin *AUX-Stecker* genannt wird und der das Mainboard zusätzlich mit 3,3- und 5,0-Volt-Spannung versorgt (Abbildung 7.21). Dieser Stecker basierte auf dem Stromstecker der AT-Mainboards, dem Vorgänger von ATX.

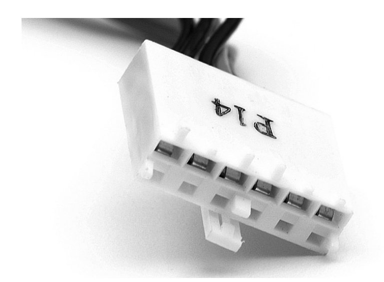


Abb. 7.21: AUX-Stromstecker

Diese beiden zusätzlichen Stromstecker brachten für die Industrie einige Kinderkrankheiten mit. Insbesondere waren Mainboards mit AMD-CPUs meist auf den AUX-Stecker angewiesen, während Mainboards mit Intel-CPUs mit dem P4 auskamen. Um Kosten zu senken, wurden viele Netzteile angeboten, die nur einen P4- oder nur einen AUX-Stecker besaßen. Das größte Problem des ATX12V-Standards war seine schwache Ausgestaltung. Es gab zwar zahlreiche Empfehlungen, aber nur wenige verbindliche Anforderungen, sodass Netzteilhersteller eine Menge Alternativen hatten (wie z.B. die wahlweise Ausstattung mit AUX- und/oder P4-Stecker). Dieser Mangel wurde erst in späteren Versionen des Standards behoben.

EPS12V Server-Mainboards sind energiehungrig und manchmal bot ATX12V 1.3 einfach zu wenig Leistung. Wichtige Vertreter der Industrie schlossen sich unter dem Namen *SSI* (*Server System Infrastructure*) zusammen und entwickelten unter dem Namen *EPS12V* ein Netzteil und ein Mainboard, die nicht dem ATX-Standard entsprachen. Ein EPS12V-Netzteil besaß einen 24-poligen Hauptstecker für das Mainboard, der zwar dem 20-poligen ATX-Stecker ähnelte, aber mehr Strom lieferte und damit für den stabilen Betrieb des Mainboards sorgen konnte. Außerdem besaß es einen AUX-Stecker, einen ATX12V-P4-Stecker und einen einzigartigen 8-poligen Stecker. EPS12V-Netzteile verfügen nicht nur über eine Menge Stecker, sondern sind auch nicht mit ATX12V-Netzteilen kompatibel.

EPS12V wurde zwar außerhalb des Serverbereichs kaum genutzt, führte aber etliche Funktionen ein, die schließlich zu Bestandteilen des ATX12V-Standards wurden. Die wohl wichtigste Neuerung waren dabei die sogenannten *Spannungsschienen*.

Spannungsschienen Im Allgemeinen stammt der gesamte Strom für den PC aus einem einzigen Transformator, der den Wechselstrom aus einer Steckdose aufnimmt und ihn in Gleichstrom umwandelt, der in drei primäre Gleichstromspannungsschienen aufgeteilt wird: 12,0, 5,0 und 3,3 Volt. Einzelne Leitungen führen von jeder dieser Spannungsschienen zu den verschiedenen Steckern.

Jede Schiene kann nur eine bestimmte maximale Energie zur Verfügung stellen. Normale Computer erreichen diese Grenze nur selten, aber anspruchsvolle Systeme mit hochentwickelten Prozessoren und Grafikkarten erfordern schnell mehr Energie, als so manche Schiene bereitstellen kann. Früher lieferten 12-Volt-Schienen rund 18 Ampere, was für Hochleistungsgeräte nicht ausreicht.

Dieses Problem wurde meistens durch den Einbau mehrerer zusätzlicher 12-Volt-Schienen in das Netzteil gelöst. Das funktioniert gut, solange die Last ordnungsgemäß auf die Schienen verteilt wird. Die Schaltung, die die Stromstärke überwacht, die durch die einzelnen Schienen fließt, die sogenannte Überstromschutzeinrichtung (Over-Current Protection, OCP), schaltet das Netzteil aus, wenn die Kapazität überschritten wird. Bei einem System mit nur einer Schiene gibt es nur eine OCP-Schaltung, bei Systemen mit mehreren Schienen besitzt jede davon eine eigene.

Bei den ersten Implementierungen von Systemen mit mehreren Schienen funktionierte die Verteilung der Stromlast nicht besonders gut. PC-Enthusiasten hatten weiterhin damit zu kämpfen, dass das System bei zu hoher Last abgeschaltet wurde. Diese Probleme sind aber seit etwa 2008 behoben. Heutzutage kommen die Netzteile mit mehreren Schienen mit fast beliebigen Lasten zurecht.

Inzwischen verbauen die Hersteller solcher Hochleistungsnetzteile 12-Volt-Schienen, die Ströme von 70 Ampere und mehr vertragen.

ATX12V 2.0 Mit *ATX12V 2.0* wurden viele der guten EPS12V-Ansätze und insbesondere der 24-polige Stecker in den ATX-Standard übernommen. Der hier definierte 24-polige Mainboard-Stromstecker ist aber abwärtskompatibel zum älteren 20-poligen Stecker, sodass man kein neues Mainboard kaufen muss, wenn man ein ATX12V-2.0-Netzteil einsetzen will. ATX12V 2.0 schreibt für alle Netzteile mit mehr als 230 Watt Leistung zwei 12-Volt-Schienen vor. Darüber hinaus entfiel mit ATX12V 2.0 der AUX-Stecker, während SATA-Stecker nun vorgeschrieben waren.

Bei vielen ATX12V-2.0-Netzteilen gibt es Adapter, die den 24-poligen in einen 20-poligen Stecker umwandeln. Das ist praktisch, wenn Sie »saubere« Verbindungen herstellen wollen, weil die 20-poligen Stecker häufig das Einstecken eines 24-poligen Steckers verhindern. Oftmals wird für die 24-poligen Stecker auch eine Bauart verwendet, bei der die zusätzlichen vier Pins nur angesteckt sind und damit auch entfernt werden können. Abbildung 7.22 zeigt die beiden Stecker und in Abbildung 7.23

sehen Sie einen konvertierbaren Stecker. Obwohl sie ähnlich aussehen, können die Stecker mit den zusätzlichen vier Pins keinen P4-Stecker ersetzen. Sie sind nicht kompatibel!

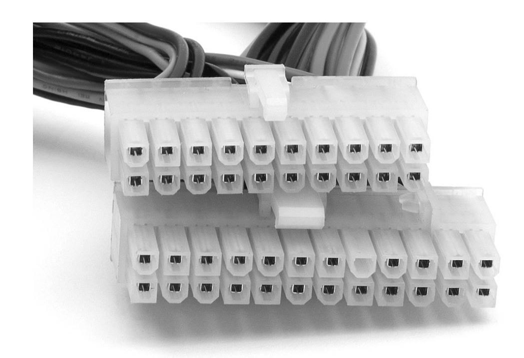


Abb. 7.22: 20- und 24-polige Stecker



Abb. 7.23: Wandlungsfähiger Mainboard-Stromstecker

Auf vielen modernen ATX-Mainboards gibt es einen 8-poligen CPU-Stromanschluss, der dem aus dem EPS12V-Standard ähnelt und stromhungrige High-End-Prozessoren mit zusätzlichem Strom versorgen soll. Dieser Anschluss wird unterschiedlich genannt, wie z.B. *EPS12V*, *EATX12V* oder auch *ATX12V 2x4*. Die eine Hälfte des Steckers ist dabei pinkompatibel mit dem P4-Stromanschluss, während die andere mit einer Schutzkappe versehen werden kann. Aus dem Mainboard-Handbuch sollten Sie jedenfalls erfahren können, ob alle acht Pins benötigt werden. Um abwärtskompatibel zu bleiben, gibt es bei einigen Netzteilen 8-polige Stromstecker, die sich in zwei 4-polige aufteilen lassen. Bei einem der beiden Stecker handelt es sich dann um einen P4-Stecker.

Ein weiterer erwähnenswerter Stecker ist der 6-polige PCIe-Stromstecker (PCI Express), der in Abbildung 7.24 gezeigt wird. Einige Mainboards besitzen einen zusätzlichen Molex-Anschluss für PCIe, und vereinzelt finden Sie Molex-Anschlüsse auch auf Steckkarten. Leistungsfähigere Grafikkarten besitzen häufig speziell dafür vorgesehene 6- oder 8-polige PCIe-Stromanschlüsse. Dabei sollte der 8-polige PCIe-Anschluss nicht mit dem inkompatiblen EPS12V-Anschluss verwechselt werden. Einige PCIe-Steckkarten mit dem 8-poligen Anschluss lassen stattdessen auch die Verwendung der 6-poligen PCIe-Stromstecker zu, können dann aber möglicherweise nicht ihre volle Leistung entfalten. Häufig begegnen Sie auch 8-poligen PCIe-Stromkabeln, bei denen sich zwei der Pins leicht entfernen lassen, sodass sie letztlich auch mit Komponenten kompatibel sind, bei denen die 6-poligen Anschlüsse verwendet werden.

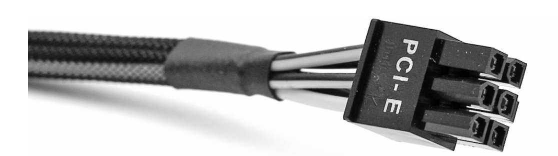


Abb. 7.24: 6-poliger PCI-Express-Stromstecker

Nischenmarkt Netzteil-Formfaktoren Die Nachfrage nach kleineren und leiseren PCs hat zur Entwicklung verschiedener Netzteil-Formfaktoren in einem Nischenmarkt geführt. Sie alle verwenden zwar die standardisierten ATX-Stecker, unterscheiden sich aber hinsichtlich Form und Größe von ATX-Netzteilen.

Einige der verbreiteteren speziellen Netzteilvarianten sind:

- **Mini-ITX und micro-ATX**: Ein kleinerer Netzteil-Formfaktor, der speziell für Mini-ITX- bzw. micro-ATX-Gehäuse ausgelegt ist.

- **TFX12V**: Ein kleiner Netzteil-Formfaktor, der für flache ATX-Systeme optimiert ist.
- **SFX12V**: Ein kleiner Netzteil-Formfaktor, der für Systeme mit FlexATX-Mainboards optimiert ist (Abbildung 7.25).

Hinweis

Häufig werden die Netzteile aus diesem Nischenmarkt zusammen mit Computergehäusen (und oft auch Mainboards) verkauft. Komponenten mit diesen Formfaktoren werden nur selten einzeln verkauft.



Abb. 7.25: SFX-Netzteil

Aktive Leistungsfaktorkorrektur (Active PFC) Stellen Sie sich den Wechselstrom vom Stromversorger wie Wasser in einem Rohr vor, das 50-mal in der Sekunde gleichmäßig vor und zurück schwappt. Ein PC-Netzteil, das diesen Wechselstrom einfach in Gleichstrom umwandelt, lässt sich mit jemandem vergleichen, der mit einem Strohhalm am Ende des Rohrs saugt. Wasser bekommt er nur dann zu trinken, wenn das Wasser am Anfang oder Ende eines Zyklus seinen vollen Druck entfaltet. Gleichzeitig entsteht eine Art Rückdruck und damit kommt es zu kleineren Störwellen, die auch *Oberschwingungen* genannt werden. Diese Oberwellen sorgen für den hörbaren Brummton, den manche elektrischen Geräte erzeugen. Mit der Zeit können diese Störwellen elektrische Bauteile beschädigen und beim Netzteil oder anderen elektrischen Komponenten im Stromkreis zu ernsthaften Problemen führen. Wenn Sie ein paar Tausend PCs mit Netzteil am selben Ort aufstellen, können derartige Oberschwingungen sogar die Anlagen des Stromversorgers beschädigen!

Gute Netzteile verfügen über zusätzliche Schaltungen zur *aktiven Leistungsfaktorkorrektur* (*Active PFC – Active Power Factor Correction*), die den Transformationsprozess regeln und die Störwellen glätten. Jedenfalls sollten Sie kein Netzteil ohne aktive Leistungsfaktorkorrektur kaufen. Normalerweise finden Sie entsprechende Angaben auf der Verpackung des Netzteils (Abbildung 7.26).

Tipp

Zu Kapitel 7 gibt es unter `http://totalsem.com/100x` wieder eine Übung, bei der Stromstecker erkannt werden müssen. Probieren Sie es aus!


Antec®
The Power of You

[ENGLISH] Model: Neo HE 550

- **ATX12V v2.2 and EPS12V compliant.**
- **Dual CPU and dual core ready.**
- **Advanced cable management system** improves internal airflow and reduces system clutter by allowing you to use only the cables that you need.
- **Universal Input** automatically accepts line voltages from 100V to 240V AC.
- **Active PFC** (Power Factor Correction) delivers environmentally-friendlier power.
- **Up to 85% efficiency** reduces heat generation and saves power and money.
- **Dedicated voltage outputs** to deliver more stable power.
- **Voltage feedback** and tight ±3% regulation for improved system stability.
- **Three +12V output circuits** provide maximum stable power for the CPU independently and for other peripherals.
- **Dual PCI Express** graphics card power connectors.
- **Low-speed 80mm fan** delivers whisper-quiet cooling and ensures quiet operation by varying fan speed in response to load and conditions.

Abb. 7.26: Netzteil mit Active PFC

Die Wattleistung

Alle Komponenten im PC benötigen eine gewisse *Wattleistung*, um funktionieren zu können. Eine typische Festplatte benötigt bei einem Zugriff z.B. ca. 15 Watt, während ein Vierkern-Intel i7-4790K bei voller Auslastung satte 151 Watt benötigt. Die gesamte Leistungsaufnahme aller Komponenten ist die minimale Wattleistung, die vom Netzteil bereitgestellt werden muss.

Wenn Sie ein Netzteil für ein System auswählen, sollten Sie sich vergewissern, dass es genügend Leistung liefern kann, um alle im System verbauten Komponenten mit Energie zu versorgen. Zudem muss das Netzteil auch alle Gerätetypen unterstützen, die im System vorhanden sind. Erst neulich habe ich eine Grafikkarte durch eine neue ersetzt, die anstelle eines einzelnen 6-poligen Kabels zwei 8-polige benötigt (Abbildung 7.27). Das Netzteil muss diese Verbindung natürlich bereitstellen.

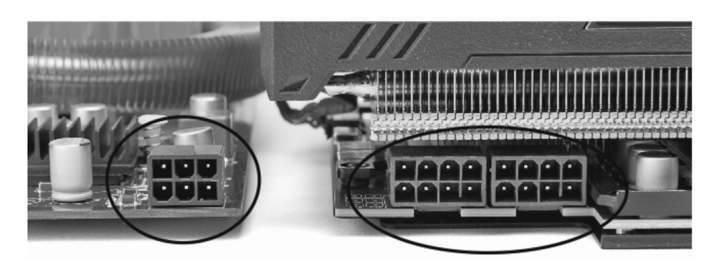


Abb. 7.27: Zwei völlig verschiedene Spannungsversorgungen!

Wenn das Netzteil die von einem System benötigte Leistung nicht liefern kann, dann arbeitet der entsprechende PC nicht korrekt bzw. unzuverlässig. Da die meisten Komponenten im PC die höchste Leistung beim ersten Einschalten benötigen, führen zu schwache Netzteile meist zu großen Briefbeschwerern, die wie ein PC aussehen. Das kann zu ziemlich abstrusen Situationen führen. So können

Sie z.B. bei einem Kunden eine neue Festplatte anschließen, den Rechner einschalten und feststellen, dass nichts mehr passiert und der Rechner tot zu sein scheint. Autsch! Sie können leicht feststellen, ob das Problem durch fehlende Netzteilleistung verursacht wird. Trennen Sie das neu eingebaute Laufwerk von der Stromversorgung und schalten Sie das System wieder ein. Startet es nun wieder, steht das Netzteil in Verdacht. Das Problem lässt sich dann nur durch Einbau eines leistungsfähigeren Netzteils beheben (oder durch Verzicht auf die neue Festplatte, was aber kaum erwünscht sein dürfte).

Hinweis

Ein unterdimensioniertes Netzteil muss einen PC nicht unbedingt vollständig lahmlegen. So gibt es beispielsweise Grafikkarten, die eigentlich mehr Leistung benötigen, die jedoch weiterarbeiten, aber mit verringerter Bildwiederholfrequenz. Spiele laufen dann nicht ordentlich, aber der Computer funktioniert zumindest. Mehr zu energiehungrigen Grafikkarten finden Sie in Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*.

Kein Netzteil kann 100 Prozent des Wechselstroms vom Stromversorger in Gleichstrom umwandeln. Alle Netzteile versorgen das System also mit weniger Leistung als der Steckdose entnommen wird. Die Differenz geht durch Abwärme verloren. Wie viel verloren geht, steht auf der Geräteverpackung. Die ATX12V-2.0-Standards fordern, dass der Wirkungsgrad des Netzteils mindestens 70 Prozent beträgt, aber es gibt auch viele Netzteile, bei denen er über 80 Prozent liegt.

Der Wirkungsgrad von Netzteilen wird typischerweise anhand eines Standards namens *Plus 80* beurteilt, dem sich die Hersteller freiwillig unterwerfen. Die Bewertungen reichen von 80 bis 94 Prozent und werden durch eine vordefinierte Last ermittelt. Die Bezeichnungen der Wirkungsgrade ähneln denen von Metallen, wie z.B. Bronze (85 Prozent), Gold (90 Prozent) oder Titanium (94 Prozent). Diese Wirkungsgrade der Netzteile werden bei Bereitstellung einer eng eingegrenzten Wattleistung erzielt. Bei höherer oder niedriger Leistungsaufnahme sind die Geräte weniger effizient. In der Dokumentation des Netzteils finden sich für gewöhnlich Diagramme, aus denen der Wirkungsgrad bei einer bestimmten Leistungsaufnahme hervorgeht. Daran erkennen Sie, wie viel Watt das System beim tatsächlichen Einsatz an den PC weitergibt. Darüber hinaus bedeutet der verbesserte Wirkungsgrad, dass das Netzteil weniger Strom verbraucht und Ihnen Geld sparen hilft.

Wichtig

In den CompTIA A+-Zertifizierungsprüfungen müssen Sie nicht die von bestimmten Systemen benötigte exakte Wattleistung berechnen können. Wenn Sie aber selbst einen PC für einen Kunden zusammenstellen, sollten Sie diese kennen!

Ein häufig gehörtes Argument lautet, dass durch den Kauf zu groß dimensionierter Netzteile für ein System Strom vergeudet wird. Das stimmt aber nicht. Ein Netzteil stellt nur den vom System wirklich benötigten Strom bereit. Wenn Sie ein 1.500-Watt-Netzteil in ein System einbauen, das nur 250 Watt benötigt, liefert das Netzteil dem System auch nur diese 250 Watt. Der Kauf eines effizienten Netzteils mit hoher Wattleistung bringt Ihnen also zwei Vorteile: Erstens hält das Netzteil länger, wenn es nicht immer unter Volllast läuft, und zweitens stehen Ihnen genügend Reserven für den Einbau weiterer Komponenten zur Verfügung.

Halten Sie die Netzteilleistung nicht zu knapp. Die Leistungsabgabe von Netzteilen sinkt durch den Verschleiß ihrer internen Komponenten mit der Zeit. Wenn Sie ein System aufbauen, das nur ein paar Watt weniger braucht, als das Netzteil anfangs liefern kann, dann werden Sie spätestens ein Jahr später Probleme bekommen. Tun Sie sich selbst und Ihren Kunden den Gefallen und verwenden Sie Netzteile, die immer etwas mehr Leistung als nötig liefern.

Generell empfehle ich bei neuen Systemen mindestens den Einbau eines 500-Watt-Netzteils. Derartige Netzteile sind recht gebräuchlich und bieten darüber hinaus genügend Leistungsreserven für zukünftige Erweiterungen.

Tipp: Leistungsbedarf berechnen

Im Internet sind einige tolle Tools verfügbar, mit denen Sie den Leistungsbedarf für bestimmte Computersysteme berechnen können. Wie eben erwähnt, habe ich kürzlich eine Grafikkarte durch eine sehr hochwertige Grafikkarte für Spiele ersetzt (und ein zweites SSD-Laufwerk eingebaut, damit mehr Speicherplatz verfügbar ist). Deshalb musste ich feststellen, ob ich für ein stabil laufendes System auch ein neues Netzteil benötigte. Sie werden als Techniker in die gleiche Situation geraten.

Starten Sie einen Webbrowser und sehen Sie sich unter `https://outervision.com/power-supply-calculator` den Rechner für die erforderliche Leistung von Netzteilen an. Geben Sie die Einzelheiten des erwünschten Systems ein und lassen Sie den Rechner die Berechnung erledigen. Der Rechner liefert auch Informationen zur Energieeffizienz und spricht eine Kaufempfehlung aus (und zwar nicht für Produkte von Outer Vision). Es handelt sich hier um ein wirklich raffiniertes und komfortables Tool. Erstellen Sie ein Lesezeichen!

7.3 Netzteile einbauen, warten und prüfen

Bei der Installation, Wartung und Prüfung von Netzteilen muss man zwar weniger rechnen als bei der Auswahl des richtigen Netzteils für ein bestimmtes System, aber dennoch sollte jeder Techniker diese Aufgabe beherrschen. Der Einbau dauert nicht lange und die Wartung ist fast genauso einfach. Lesen Sie dazu die nächsten Abschnitte.

7.3.1 Einbau

Das typische Netzteil ist mit vier der bei Computern üblichen Schrauben hinten im PC-Gehäuse befestigt (Abbildung 7.28). Wenn Sie die vier Schrauben entfernen, können Sie das Netzteil einfach entnehmen (Abbildung 7.29). Setzen Sie ein neues Netzteil ein, das in das Gehäuse passt, und befestigen Sie es wieder mit den vier Schrauben.



Abb. 7.28: Befestigungsschrauben des Netzteils



Abb. 7.29: Entfernen des Netzteils aus der Systemeinheit

Der Umgang mit ATX-Netzteilen erfordert eine besondere Vorgehensweise. Sie wissen, dass ein ATX-Netzteil *nie ausgeschaltet* ist. Solange ein solches Netzteil an eine Steckdose angeschlossen ist, versorgt es das Mainboard laufend mit einer Spannung von 5 Volt. Trennen Sie ein ATX-System immer von der Stromversorgung, wenn Sie Arbeiten darin vornehmen wollen. Jahrelang haben Techniker darüber gestritten, ob man den Rechner bei der Arbeit besser an der Stromversorgung hängen lässt oder nicht. Seit ATX ist diese Frage geklärt. Viele ATX-Netzteile haben an ihrer Rückseite einen echten Netz-

schalter (Abbildung 7.30). Wenn Sie dafür sorgen wollen, dass das Mainboard wirklich nicht mehr mit Strom versorgt wird, dann benutzen Sie diesen Schalter.



Abb. 7.30: Netzschalter eines ATX-Systems

Wenn Sie an einem ATX-System arbeiten und das Gehäuse nicht verwenden oder die Leitungen des Netzschalters noch nicht mit dem Mainboard verbunden haben, kann die Benutzung des Netzschalters unpraktisch sein, da es einen solchen dann gar nicht gibt. Sie können sich aber mit einem Trick behelfen. Schließen Sie dann einfach die beiden Kontakte für das Ein- und Ausschalten des Systems mit einem Autoschlüssel oder einem Schraubendreher kurz (Abbildung 7.31).

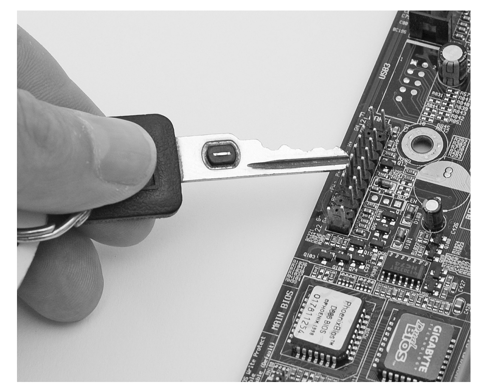


Abb. 7.31: Kurzschließen des Softpower-Jumpers

Nach dem Kauf eines neuen Netzteils müssen Sie zunächst prüfen, ob es funktioniert. Verbinden Sie die Stromstecker mit dem Mainboard, bevor Sie das System starten. Werden Grafikkarten mit eigenen Stromanschlüssen verwendet, schließen Sie diese ebenfalls an. Andere Stecker, wie z.B. für Festplatten, können noch bis nach dem ersten Teststart warten. Und wenn Sie ein wenig übermütig sind, schließen Sie einfach alles sofort an!

7.3.2 Kühlung

Wärme und Computer sind nicht gerade die besten Freunde. Beim Aufbauen oder Zusammenstellen eines Computers muss daher für ausreichende Kühlung gesorgt werden. Elektrizität erzeugt Wärme. Computer sind Elektrogeräte und erzeugen bei ihrer Arbeit Wärme. Werden die Komponenten aber zu warm, dann können sie schweren Schaden nehmen.

Der Netzteillüfter (Abbildung 7.32) sorgt für die grundlegende Kühlung des Rechners. Er kühlt nicht nur die Spannungsregler im Netzteil selbst, sondern sorgt auch für die gleichmäßige Luftzirkulation im

Innern des Rechnergehäuses. Wenn er einmal ausfallen sollte, kann dies schnell zu erheblichen Problemen und defekten Komponenten führen. Wenn Sie einen Rechner einschalten, der zwar ordnungsgemäß bootet, aber ungewöhnlich leise zu sein scheint, dann sollten Sie nachsehen, ob der Netzteillüfter noch funktioniert. Sollte er defekt sein, schalten Sie den Rechner sofort ab und ersetzen Sie das Netzteil!



Abb. 7.32: Der Lüfter eines Netzteils

Einige Netzteile enthalten einen Temperaturfühler, der den Luftstrom reguliert. Wird das System warm, dreht sich der Netzteillüfter schneller (Abbildung 7.33).

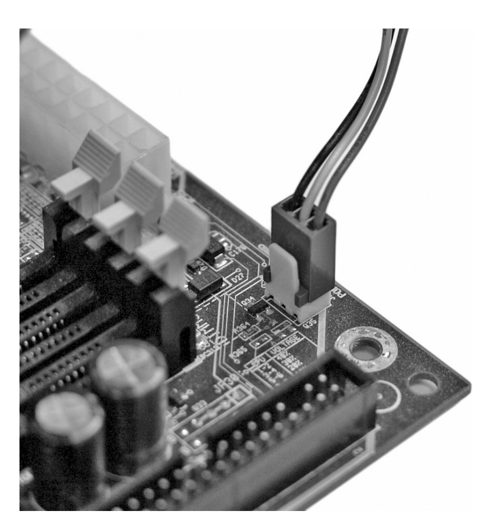


Abb. 7.33: Anschluss für den 3-poligen Stecker des Temperaturfühlers

Gehäuselüfter (Abbildung 7.34) sind große, quadratische Lüfter, die in bzw. an Aussparungen des Gehäuses oder direkt am Gehäuse montiert werden und für zusätzliche Kühlung der wesentlichen Komponenten sorgen. Die meisten Gehäuse enthalten bereits einen Gehäuselüfter, und moderne Computer sollten unbedingt einen oder zwei davon haben.

Die wichtigste Frage, die sich im Zusammenhang mit Gehäuselüftern stellt, ist die nach deren Anschluss. Die meisten Gehäuselüfter besitzen herkömmliche Molex-Stecker, die leicht angeschlossen werden können. Andere Lüfter besitzen aber spezielle 3-polige Stromstecker, die mit entsprechenden Anschlüssen auf dem Mainboard verbunden werden müssen. Es sind aber auch Adapter erhältlich, mit denen sich diese beiden Anschlussvarianten ineinander überführen lassen.

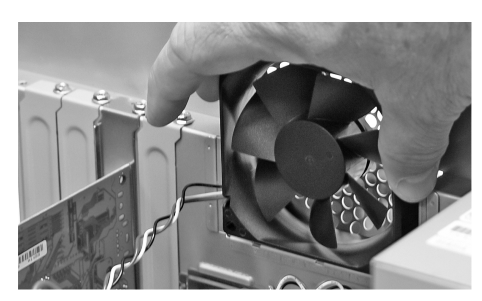


Abb. 7.34: Ein Gehäuselüfter

Gute Luftzirkulation

Computer sind geschlossene Systeme und Computergehäuse unterstützen die Lüfter bei ihrer Arbeit: Alle Komponenten befinden sich im Innern des Gehäuses. Und auch wenn viele Techniker ihr System lieber mit abgenommenem Seitenteil betreiben, damit die Komponenten besser zugänglich bleiben, machen sie sich damit doch selbst etwas vor. Warum? Im geschlossenen Gehäuse sorgen die Lüfter dafür, dass die Luft zirkuliert. Im Luftzug werden die internen Komponenten besser gekühlt. Bei abgenommenem Seitenteil ist aber die Luftzirkulation im System beeinträchtigt, sodass es weit weniger wirksam gekühlt wird.

Wenn Sie für eine gute Luftzirkulation im Rechnergehäuse sorgen wollen, dann sollten Sie nicht vergessen, dass warme Luft nach oben steigt und sich damit im Gehäuse letztlich über der kalten Luft befindet. Sie können dieses Prinzip bei der Kühlung des Rechners zum eigenen Vorteil nutzen.

Bei der typischen Anordnung von Lüftern in einem Rechnergehäuse befindet sich ein Lüfter, der kalte Luft von außen in das Gehäuse und über die Komponenten bläst, unten an der Vorderseite des Gehäuses. Ziemlich weit oben und an der Rückseite des Gehäuses (normalerweise in der Nähe des Netzteils) befinden sich Lüfter, die (warme) Luft aus dem Gehäuse nach außen befördern.

Weiterhin wichtig für die richtige Luftzirkulation im Gehäuse ist, dass alle leeren Erweiterungssteckplätze mit *Slotblechen* verschlossen werden (Abbildung 7.35). Damit die Luft im Gehäuse möglichst gut zirkulieren kann, sollte sie nicht an allzu vielen Stellen entweichen können. Slotbleche unterstützen nicht nur die gleichmäßige Luftzirkulation, sondern sorgen auch dafür, dass Staub und Rauch nicht in das Gehäuse gelangen.



Abb. 7.35: Slotblech

Wichtig

Fehlende Slotbleche können zu einer Überhitzung des Rechners führen!

Reduzierung der Lüftergeräusche

Lüfter verursachen Lärm. Beim Versuch, für eine ausreichende Kühlung zu sorgen, bauen viele Techniker mehrere Hochgeschwindigkeitslüfter in ein Gehäuse ein, sodass sich der PC wie ein Düsentriebwerk anhört. Sie können den Lüfterlärm reduzieren, indem Sie Lüfter mit manuell einstellbarer Geschwindigkeit, größere Lüfter oder spezielle leise Lüfter verwenden. Bei vielen Mainboards lässt sich die Lüfterdrehzahl über Software steuern.

Manuell einstellbare Lüfter besitzen einen kleinen Drehregler zur Steuerung der Geschwindigkeit (Abbildung 7.36). Mit derartigen Lüftern lässt sich der Lärm zwar reduzieren, aber Sie laufen dann Gefahr, den Lüfter zu weit abzubremsen und damit das Gehäuseinnere zu heiß werden zu lassen. Eine bessere Lösung sind leisere Lüfter.



Abb. 7.36: Komponente zur manuellen Anpassung der Lüfterdrehzahl

Größere Lüfter drehen sich langsamer, sodass sie bei ausreichender Luftzirkulation leiser laufen. Die Lüfterabmessungen werden in Millimetern (mm) oder Zentimetern (cm) angegeben. Traditionell wurden auch in Netzteilen 80-mm-Lüfter verwendet. Heute gibt es aber auch 100- und 120-mm-Lüfter (oder noch größere) in Netzteilen und für den Einbau in das Rechnergehäuse.

Viele Unternehmen stellen hochwertigere, leisere Lüfter her. Die Lüfter besitzen bessere Lager als die Standardlüfter, deshalb kosten sie etwas mehr, aber sie sind ihren Preis eindeutig wert. Die Lüfter tragen häufig Bezeichnungen wie beispielsweise »leise« oder »still«. Wenn Sie auf einen PC treffen, der sich anhört, als würde er jeden Moment abheben, versuchen Sie, die Gehäuselüfter durch einen leisen Lüfter von *Papst*, *NZXT* oder *Cooler Master* auszutauschen. Entscheiden Sie sich anhand der Dezibel-Angabe für ein Modell. Je niedriger, desto besser. Beachten Sie auch, dass der Typ des Lagers einen Unterschied macht. Lüfter mit einem Gleitlager werden mit der Zeit lauter. Das ist bei Lüftern mit einem Kugellager nicht der Fall. Der Preisunterschied ist minimal, entscheiden Sie sich also immer für Kugellager.

Weil sich die Temperatur innerhalb eines PCs abhängig von seiner Belastung ändert, wird bei der besten Lösung ein guter Lüftersatz mit Temperatursensoren zur automatischen Regelung verwendet. Ein gerade untätiger PC benötigt nur halb so viel Strom wie ein PC, auf dem ein grafikintensives Computerspiel läuft, und wird deshalb auch weniger warm. Fast alle modernen Systeme unterstützen drei Lüfter, die mit drei 3-poligen Lüfteranschlüssen auf dem Mainboard verbunden werden können. Der CPU-Lüfter verwendet einen dieser Stecker, aber die beiden anderen sind für Gehäuse- oder Netzteillüfter vorgesehen.

Über die meisten CMOS-Setups lassen sich die an das Mainboard angeschlossenen Lüfter rudimentär überwachen. Abbildung 7.37 zeigt die typischen CMOS-Einstellungen für die Lüfter. Beachten Sie, dass sich die Lüfter hier nicht ein- oder ausschalten lassen. Sie können hier nur Werte für die Temperatur oder die Drehzahl angeben, bei denen ein Alarm ausgelöst werden soll.

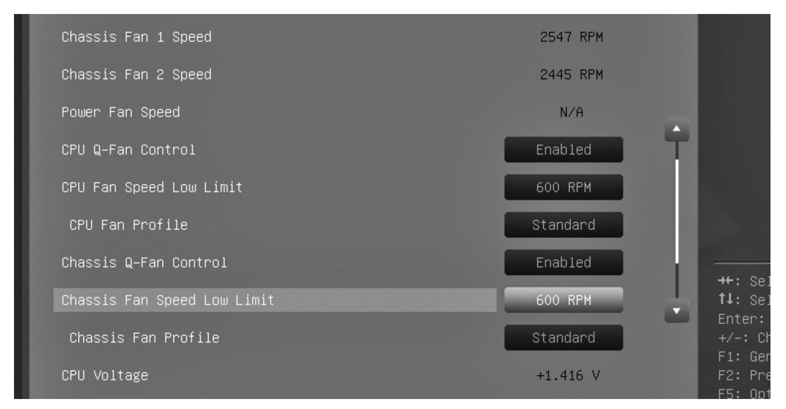


Abb. 7.37: CMOS-Optionen für die Lüfter

Am besten steuern Sie Lüfter per Software. Einigen Mainboards liegen Programme zur Systemüberwachung bei, mit der Sie die Temperaturen einstellen können, bei denen die Lüfter anlaufen bzw. anhalten sollen. Wenn Ihrem Mainboard kein solches Programm beilag und auf der Website des Herstellers auch kein solches zum Download angeboten wird, dann können Sie das beliebte Freeware-Dienstprogramm *SpeedFan* von Alfredo Milani Comparetti ausprobieren (Abbildung 7.38), das die Spannungen, Lüfterdrehzahl und Temperaturen in Computern mit installierten Hardwareüberwachungschips beobachtet. SpeedFan kann bei Festplatten, die diese Funktion unterstützen, sogar auf die S.M.A.R.T.-Informationen (siehe Kapitel 8, *Festplattentechnologien*) zugreifen und die Festplattentemperatur anzeigen. Sie finden SpeedFan unter `http://www.almico.com/speedfan.php`.

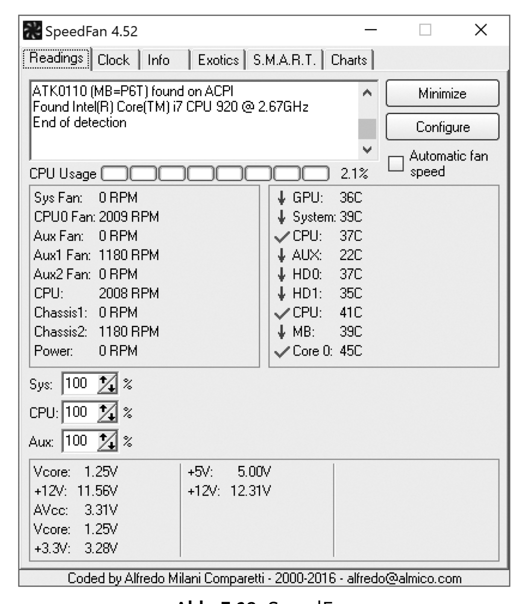


Abb. 7.38: SpeedFan

Vorsicht

SpeedFan ist ein leistungsfähiges Werkzeug, das weit mehr als nur die Lüftersteuerung unterstützt. Ändern Sie aber nichts an Einstellungen, deren Bedeutung Ihnen nicht klar ist!

Auch wenn Sie sich nicht weiter mit den Lüftern befassen wollen, sollten Sie den Temperaturalarm im CMOS immer aktivieren. Sie werden dann gewarnt, wenn das System zu heiß wird. Nur anhand eines rechtzeitig ausgelösten Alarms können Sie erkennen, dass ein Lüfter nicht mehr funktioniert!

7.4 Fehlersuche bei Netzteilen

Netzteile fallen entweder plötzlich oder ganz allmählich aus. Wenn sie plötzlich ausfallen, dann startet der Rechner nicht und auch der Lüfter im Netzteil dreht sich nicht mehr. Überzeugen Sie sich dann aber erst einmal davon, dass das Netzteil auch wirklich mit Strom versorgt wird, bevor Sie irgendwelche anderen Maßnahmen ergreifen! Wenn lediglich die Steckdose defekt oder ein Verlängerungskabel nicht eingesteckt ist bzw. der Stecker am Netzteil nicht richtig sitzt, dann können Sie sich dadurch viel Zeit und Ärger sparen. Sofern das Netzteil ordnungsgemäß mit Strom versorgt wird, prüfen Sie am besten mit einem Multimeter die vom Netzteil abgegebenen Spannungen (Abbildung 7.39).



Abb. 7.39: Prüfen einer 5-Volt-Gleichstromleitung

Machen Sie sich keine Sorgen, falls Sie beim Messen feststellen, dass das Netzteil etwas mehr oder weniger als die nominale Spannung liefert. Die von den meisten PC-Netzteilen gelieferten Spannungen dürfen vom Sollwert um bis zu 10 Prozent nach oben oder unten abweichen. Die gemessene Spannung einer 12-Volt-Leitung kann also zwischen ungefähr 10,8 und 13,2 Volt liegen, ohne die zulässigen Toleranzen zu überschreiten. Für die 5- und 3,3-Volt-Leitungen gelten ähnliche Toleranzen.

Überprüfen Sie immer alle einzelnen Anschlüsse und Leitungen des Netzteils, also auch alle Molex- und Mini-Molex-Stecker. Stellen Sie zu diesem Zweck das Voltmeter auf einen Messbereich von 20 Volt Gleichspannung (DC) ein, um den Bereich zwischen -20 und +20 Volt messen zu können. Falls das Netzteil keine Spannung liefert, überantworten Sie es dem Sondermüll, und zwar auch dann, wenn Sie sich zu den Hardwareexperten zählen und einen Lötkolben zu benutzen wissen. Angesichts des Preises neuer Netzteile sollten Sie Ihre Zeit nicht mit derartigen Bastelarbeiten verschwenden!

Hinweis

Mit vielen CMOS-Setup-Programmen oder anderen Dienstprogrammen lassen sich ebenfalls die verschiedenen Spannungen anzeigen. Das erspart Ihnen den Einsatz eines Multimeters. Natürlich muss der PC noch so weit funktionieren, dass Sie ins CMOS-Setup-Programm gelangen können.

7.4.1 Kein Mainboard

Moderne PC-Netzteile funktionieren nicht, wenn sie nicht an ein Mainboard angeschlossen sind. Was machen Sie also, wenn Ihnen für den Test kein zuverlässiges Mainboard zur Verfügung steht? Verwenden Sie doch einen *ATX-Tester*. Derartige Geräte werden von vielen Unternehmen hergestellt. Suchen

Sie nach einem Modell, das 20- und 24-polige Mainboard-Stecker sowie alle anderen Stecker auf Ihrem Mainboard unterstützt. Abbildung 7.40 zeigt einen Netzteil-Tester.



Abb. 7.40: ATX-Netzteil-Tester

Wichtig

Vergewissern Sie sich, dass Ihnen Werkzeuge zur Überprüfung von Spannungen, wie Multimeter oder Netzteil-Tester, vertraut sind.

7.4.2 Schalter

Mitunter sind defekte Schalter die Ursache für ausfallende Netzteile. Der Netzschalter verbirgt sich hinter dem Ein/Aus-Schalter, den es bei allen Rechnern gibt. In der Regel ist er an der Frontabdeckung oder vorn am Gehäuse im Innern des Rechners befestigt und daher nicht gerade leicht zugänglich. Schließen Sie, wie bereits beschrieben, versuchsweise die Softpower-Jumper kurz. Verwenden Sie dazu einen Schlüssel oder einen Schraubendreher.

7.4.3 Wenn Netzteile langsam dahinsiechen

Dieses Kapitel wäre sicher kürzer ausgefallen, wenn Netzteile grundsätzlich plötzlich ausfallen würden. Leider werden aber weitaus mehr PC-Probleme von allmählich ihren Geist aufgebenden Netzteilen verursacht. Dabei baut ein elektronisches Bauteil im Netzteil langsam ab. Fehlfunktionen dieser Art treten *immer* unregelmäßig auf und sorgen für eines der am schwierigsten zu diagnostizierenden Probleme im Bereich der PC-Reparatur. Das Geheimnis beim Identifizieren des Netzteils als Schuldigem liegt in der Nichtreproduzierbarkeit. Bei unregelmäßig auftretenden Problemen sollte Ihre erste Vermutung in Richtung eines defekten Netzteils gehen. Es folgen einige weitere Anzeichen, von denen Anwender zu berichten wissen:

- »Wenn ich morgens meinen PC starte, bootet er zwar, hängt sich dann aber auf. Wenn ich dann zwei- oder dreimal `Strg` + `Alt` + `Entf` drücke, bootet er wieder normal.«
- »Manchmal wird beim Start meines Rechners ein Fehlercode angezeigt, der nach dem nächsten Start wieder verschwunden ist. Gelegentlich werden auch unterschiedliche Fehlermeldungen angezeigt.«
- »Mein Computer läuft etwa eine Stunde lang völlig normal. Dann hängt er sich auf, manchmal ein- oder zweimal in der Stunde.«
- »Ich muss ein USB-Gerät mehrmals ein- und ausstöpseln, damit mein System es erkennt.«

Manchmal gibt es heftige Probleme und zeitweise dann wieder gar keine. Genau das ist ein Hinweis auf einen nötigen Austausch des Netzteils. Und kümmern Sie sich in diesem Fall nicht um das Voltme-

ter, denn Sie werden nur Spannungen innerhalb des Toleranzbereichs messen. Die unregelmäßig auftretenden Fehler werden von kurzzeitigen Spannungsschwankungen verursacht, die sich mit einem Voltmeter nicht messen lassen. Falls Sie sich nicht sicher sind, sollten Sie das Netzteil besser auswechseln. Netzteile sind im PC mit Ausnahme von Komponenten mit beweglichen Teilen am häufigsten von Problemen betroffen. Für Testzwecke und den möglichen Austausch sollten Sie daher immer Netzteile auf Lager haben.

7.4.4 Sicherungen und Brandschutz

Im Innern aller Netzteile befindet sich eine einfache Sicherung. Wenn ein Netzteil einfach »Klick« macht und seine Arbeit einstellt, dann könnten Sie der Versuchung unterliegen, das Netzteil zu öffnen, um die Sicherung zu prüfen. Das ist keinesfalls ratsam. Zunächst einmal können Kondensatoren in den meisten Netzteilen Ladungen sehr hoher Spannung auch über einen längeren Zeitraum hinweg halten und Ihnen reichlich schmerzhafte elektrische Schläge verpassen. Und zweitens gibt es ja schließlich einen Grund dafür, dass die Sicherung durchgebrannt ist. Wenn ein Netzteil nicht mehr richtig funktioniert, dann kann man sich nur wüschen, dass seine Sicherung durchknallt. Die Alternative wäre jedenfalls weit unangenehmer.

Unterschätzt man die elektrische Energie, führt dies irgendwann beinahe unweigerlich zur größten denkbaren Katastrophe, nämlich dem Ausbruch eines Feuers. Glauben Sie nicht, dass Ihnen das nicht passieren könnte! *Feuerlöscher* dürfen in keiner PC-Werkstatt fehlen! Sie müssen aber dafür sorgen, dass der richtige vorhanden ist. Es gibt fünf primäre Brandklassen und die Hersteller haben alle Feuerlöscher diesen *Brandklassen* zugeordnet:

- **Klasse A**: Gewöhnliche brennbare, feste Materialien, wie z.B. Holz oder Papier
- **Klasse B**: Brennbare Flüssigkeiten, wie z.B. Benzin, Lösungsmittel oder Lacke
- **Klasse C**: Brände von Gasen, wie z.B. Erdgas oder Flüssiggas, aber auch betriebsbereiter elektronischer Geräte, da bei deren Brand ebenfalls brennbare Gase freigesetzt werden können
- **Klasse D**: Brände von Metallen, wie z.B. Leichtmetallen
- **Klasse K**: Öle und Fette, z.B. in einer Fritteuse

Natürlich sollten Sie für den PC nur einen Feuerlöscher der Klasse C verwenden, sofern er einmal Feuer fangen sollte. Für welche Brandklassen sich ein Feuerlöscher eignet, wird jeweils groß und deutlich auf deren Etikett angegeben. Viele Feuerlöscher eignen sich für mehrere Brandklassen und die verbreitetsten Feuerlöscher eignen sich tatsächlich für die Brandklassen A, B *und* C und damit für alle gängigen Feuer, hinterlassen aber ihre Spuren auf gelöschten Geräten.

Wichtig

Falls Rauch aus Ihrem Netzteil dringt oder wenn Sie Brandgeruch aus dessen Inneren wahrnehmen, sollten Sie es keinesfalls weiter verwenden. Ersetzen Sie es umgehend durch ein neues Netzteil.

Jenseits von A+

Netzteile leisten wesentliche Dienste für den PC, erzeugen aus Wechselspannung Gleichspannung und kühlen das System. Aber auch diese elementare Rolle hält gewisse Personen nicht davon ab, es zu ihrem Spielzeug zu machen. Zudem stellen Server und leistungsfähige Workstations etwas andere Anforderungen als eher typische Systeme, sodass natürlich mehr Leistung benötigt wird. Gehen wir also ein wenig über die A+-Prüfungsinhalte hinaus und befassen uns mit diesen Aspekten.

7.4.5 Modulare Netzteile

Es wird immer beliebter, PCs zusammenzustellen, die sowohl innen als auch außen gut aussehen. Nicht genutzte Stromkabel, die im Rechner herumhängen, sorgen für ein weniger schönes Bild und können die Luftzirkulation beeinträchtigen. Für die Modebewussten haben die Hersteller daher modulare Netzteile entwickelt (Abbildung 7.41).



Abb. 7.41: Modulares Netzteil

Diese Netzteile mit ihren Kabelmodulen sind wirklich elegant: Sie schließen nur die Leitungen an, die vom System benötigt werden. Andererseits beschweren sich einige Techniker darüber, dass durch die Stecker der Kabelmodule zusätzliche Widerstände entstehen, durch die das Netzteil weniger wirkungsvoll arbeitet. Entscheiden Sie selbst, ob Ihnen gutes Aussehen wichtiger als ein minimal geringerer Wirkungsgrad ist.

7.4.6 Temperatur und Wirkungsgrad

Achten Sie einmal darauf, dass für manche Netzteile eine Betriebstemperatur von 25° Celsius angegeben wird, also ungefähr Zimmertemperatur. Nun leistet ein Netzteil, das bei 25° Celsius 500 Watt liefert, bei höheren Temperaturen deutlich weniger – und im Inneren des PCs ist es für gewöhnlich etwa 15° wärmer als in seiner Umgebung. Leider lassen viele Netzteilhersteller – auch diejenigen, die gute Netzteile bauen –, diese Tatsache unter den Tisch fallen.

7.5 Wiederholung

7.5.1 Fragen

1. Welche Spannung sollte ein Multimeter bei der Prüfung einer Steckdose zwischen der spannungsführenden Leitung und der Erde in Deutschland anzeigen?

   A. 230 V

   B. 120 V

   C. 0 V

   D. –120 V

2. Mit welchen Spannungen versorgt der ATX12V-P1-Anschluss das Mainboard?
   A. 3,3 V, 5 V
   B. 3,3 V, 12 V
   C. 5 V, 12 V
   D. 3,3 V, 5 V, und 12 V
3. Welche Art von Steckern wird bei hochwertigen Grafikkarten für die Stromversorgung genutzt?
   A. Molex
   B. Mini-Molex
   C. PCIe
   D. SATA
4. Joachim hat ein neues Netzteil bestellt, war aber überrascht, als es ankam, weil es einen zusätzlichen 4-poligen Stecker besaß. Um was für einen Stecker handelt es sich?
   A. P2-Stecker zum Anschließen zusätzlicher Komponenten
   B. P3-Stecker zum Anschließen von Gehäuselüftern
   C. P4-Stecker zum Anschließen an moderne Mainboards
   D. Aux-Stecker zum Anschließen an ein zweites Netzteil
5. Was sollten Sie beim Testen von Gleichstromsteckern beachten?
   A. Bei der Gleichspannung muss die Polarität beachtet werden. Die rote Prüfspitze sollte immer mit der spannungsführenden Leitung und die schwarze mit der Masseleitung verbunden werden.
   B. Bei der Gleichspannung muss die Polarität beachtet werden. Die rote Prüfspitze sollte immer mit der Masseleitung und die schwarze mit der spannungsführenden Leitung verbunden werden.
   C. Gleichspannung hat keine Polarität, sodass Sie die rote Leitung entweder mit einer spannungsführenden Leitung oder einer Masseleitung verbinden können.
   D. Gleichspannung hat keine Polarität, sodass Sie die schwarze Leitung mit einer spannungsführenden oder einer neutralen Leitung, aber nicht mit einer Masseleitung verbinden dürfen.
6. Welche Spannungen sollten die beiden spannungsführenden Leitungen an einem Molex-Stecker liefern?
   A. Rot = 3,3 V; Gelb = 5 V
   B. Rot = 5 V; Gelb = 12 V
   C. Rot = 12 V; Gelb = 5 V
   D. Rot = 5 V; Gelb = 3,3 V
7. Warum ist es sinnvoll, die Slotbleche am Rechner immer anzubringen?
   A. Um für eine optimale Luftzirkulation im Gehäuse zu sorgen.
   B. Sie halten Staub und Rauch aus Ihrem Gehäuse fern.
   C. Sowohl A als auch B ist korrekt.
   D. Fangfrage! Es macht überhaupt nichts, wenn der Steckplatz offen bleibt.
8. Ein PC-Netzteil stellt Gleichstrom in welcher Standardkonfiguration bereit?
   A. Zwei primäre Spannungsschienen, 12 Volt und 5 Volt, und einen Zusatzstecker mit 3,3 Volt
   B. Drei primäre Spannungsschienen für je 12-Volt-, 5-Volt- und 3,3-Volt-Stecker
   C. Eine primäre Spannungsschiene für je 12-Volt-, 5-Volt- und 3,3-Volt-Stecker
   D. Eine Spannungsschiene mit einem 12-Volt-Stecker für das Mainboard, eine zweite mit einem 12-Volt-Stecker für die CPU und eine dritte für die 5-Volt- und 3,3-Volt-Stecker

9. Welche Funktion von ATX-Systemen hindert Benutzer daran, das System abzuschalten, bevor das Betriebssystem heruntergefahren wurde?
   A. Mainboard-Stromstecker
   B. CMOS-Setup
   C. Ruhezustand
   D. Softpower
10. Wie viele Kontakte besitzt ein SATA-Stromstecker?
   A. 6
   B. 9
   C. 12
   D. 15

7.5.2 Antworten

1. **A.** Das Multimeter sollte bei einer korrekt verdrahteten deutschen Steckdose etwa 230 V anzeigen.
2. **D.** Der P1-Stecker eines ATX12V-Netzteils versorgt das Mainboard mit 3,3, 5 und 12 Volt.
3. **B.** Hochwertige Grafikkarten verwenden einen oder zwei 6- bzw. 8-polige(n) PCIe-Stecker.
4. **C.** Der P4-Stecker wird an das Mainboard angeschlossen, um energiehungrigere Prozessoren zu unterstützen.
5. **A.** Bei der Gleichspannung gilt es, die Polarität zu beachten. Die rote Leitung sollte immer mit der spannungsführenden Leitung und die schwarze Leitung mit der Masse (Erde) verbunden werden.
6. **B.** Die roten Leitungen eines Molex-Steckers sollten 5, die gelben 12 Volt Spannung führen.
7. **C.** Sowohl A als auch B sind korrekt. Wenn Sie die Steckplätze abdecken, sorgen Sie für optimale Luftzirkulation im Gehäuse und halten Staub und Rauch von den empfindlichen internen Komponenten fern.
8. **B.** Bei der Standardkonfiguration von PC-Netzteilen gibt es drei primäre Spannungsschienen, für je 12-Volt-, 5-Volt- und 3,3-Volt-Stecker.
9. **D.** Die Softpower-Funktion von ATX-Systemen verhindert, dass der Benutzer ein System ausschaltet, bevor das Betriebssystem heruntergefahren wurde.
10. **D.** SATA-Stromstecker sind 15-polig.

Festplattentechnologien 8

Themen in diesem Kapitel:

- Funktionsweise von Festplatten
- RAID-Verbunde
- Festplatten installieren
- Fehlersuche bei der Installation

Festplatten gehören wohl zu jenen PC-Komponenten, die am häufigsten im Mittelpunkt des Interesses stehen (bzw. die meisten Probleme bereiten!). Dafür gibt es einen guten Grund: Wenn Festplatten ausfallen, droht Datenverlust! Und wenn Daten verschwinden, müssen Sie wohl oder übel entweder Ihre Arbeit noch einmal machen oder die Daten anhand eines Backups wiederherstellen. Es ist richtig, sich um die Datensicherheit Gedanken zu machen, denn es sind Daten wie Gehaltsabrechnungen und E-Mails, die für Unternehmen oder Büros lebenswichtig sind.

Dieses Kapitel konzentriert sich auf die Funktionsweise von Festplatten. Wir beginnen mit dem inneren Aufbau und der Organisation der Festplatte. Anschließend lernen Sie die verschiedenen, heute eingesetzten Festplattentypen kennen und erfahren, wie sie mit dem PC zusammenarbeiten. Das Kapitel beschreibt, wie mehrere Festplatten mithilfe von RAID-Funktionen zusammenarbeiten können, um die Datensicherheit und/oder die Geschwindigkeit zu erhöhen. Das Kapitel endet mit ausführlichen Erläuterungen zur richtigen Installation von Laufwerken im System. Los geht's.

Geschichte und Konzepte

8.1 Funktionsweise von Festplatten

Beim Bau von Festplatten kommen heute zwei verschiedene Technologien zum Einsatz. Die herkömmliche Variante arbeitet mit beweglichen Teilen, die neuere und teurere ohne. Wir werden nun beide Varianten näher betrachten.

Hinweis

In Kapitel 9, *Vorbereitung und Wartung von Festplatten*, wird das Thema Festplatten fortgesetzt. Hier kommt das Betriebssystem mit ins Spiel und Sie erfahren, wie Sie Laufwerke für die Datenspeicherung vorbereiten und wie Sie Festplatten unter den verschiedenen modernen Betriebssystemversionen warten und austauschen können.

8.1.1 Plattenbasierte Laufwerke

Herkömmliche *Festplattenlaufwerke* (*HDDs – Hard Disk Drives*) bestehen aus einzelnen Scheiben bzw. *Platten* und besitzen Schreib/Leseköpfe, die sich an einem mechanischen Positionierungsarm befinden, der von einem Servomotor gesteuert wird. Die gesamte Konstruktion befindet sich in einem versiegelten Gehäuse, das das Eindringen von verschmutzter Luft aus der Umgebung verhindert (siehe Abbildung 8.1).



Abb. 8.1: Das Innere eines Festplattenlaufwerks

Die Aluminiumplatten sind mit einem magnetischen Trägermaterial beschichtet. Für jede Platte sind zwei winzige Schreib/Leseköpfe zuständig, von denen sich einer ober- und der andere unterhalb der Platte befindet (Abbildung 8.2). Oftmals werden herkömmliche HDDs auch als *magnetische Festplatten* bezeichnet.

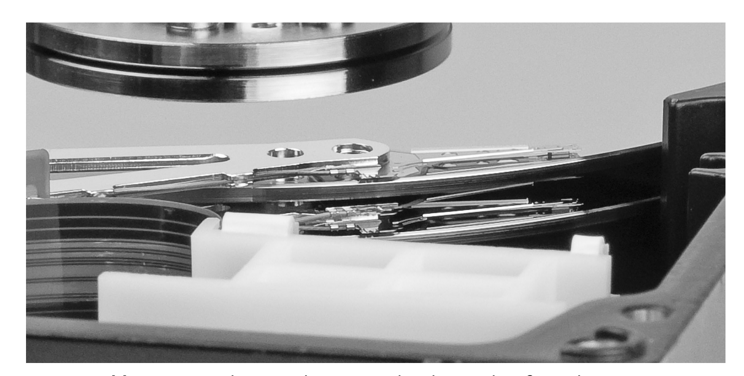


Abb. 8.2: Der obere und untere Schreib/Lesekopf mit dem Arm

1001

Rotationsgeschwindigkeit

Festplattenlaufwerke laufen mit einer Rotationsgeschwindigkeit, die in *Umdrehungen pro Minute* (U/min) angegeben wird. Alte Laufwerke rotierten standardmäßig mit 3.600 U/min, während einige der aktuellen Festplattenmodelle mit 15.000 Touren drehen. Je höher die Rotationsgeschwindigkeit, desto schneller kann der Controller Daten schreiben und lesen. Die heute üblichen Geschwindigkeiten liegen bei 5.400 und 7.200 U/min. Leistungsfähigere Laufwerke rotieren mit 10.000 und 15.000 U/min.

Schnellere Laufwerke bieten normalerweise mehr Leistung, verursachen aber auch mehr Lärm und Wärme. Wärme kann die Lebensdauer einer Festplatte drastisch verkürzen. Eine um 5° Celsius höhere Temperatur kann die Lebenserwartung einer Festplatte um bis zu zwei Jahre verringern. Wenn Sie also zwei ältere Festplatten mit 5.400 U/min durch zwei nagelneue mit 15.000 U/min ersetzen, wird aufgrund der zusätzlichen Wärme zwar nicht gleich das ganze System abstürzen, Sie setzen sich aber der Gefahr aus, schon bald wieder Geld in Speichergeräte investieren zu müssen.

Sie bekommen die Wärme dieser sehr schnellen Laufwerke in den Griff, wenn Sie zusätzliche Lüfter in Einbauschächte einsetzen oder ein voluminöseres Gehäuse verwenden. Die meisten Anhänger derartiger Laufwerke ergreifen schließlich beide Maßnahmen. Lüfter für Einbauschächte werden vor diesem Schacht angebracht und blasen Luft über das Laufwerk. Sie kosten zwischen 10 und 100 Euro und können die Temperatur der Laufwerke drastisch senken. In manchen Gehäusen sind solche, vor einem Einbauschacht angebrachte Lüfter, bereits vorinstalliert (Abbildung 8.3).

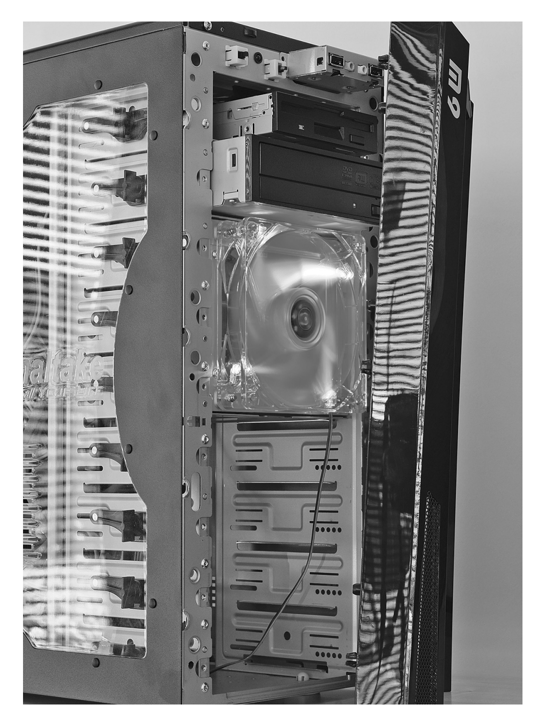


Abb. 8.3: Einbauschacht mit davor montiertem Lüfter

Die Luftzirkulation im Gehäuse kann für die Systemstabilität von entscheidender Bedeutung sein, speziell wenn Sie neue, die Umgebungstemperatur erhöhende Laufwerke installieren. Heiße Systeme werden unzuverlässig und stürzen zu den seltsamsten Zeitpunkten ab. Viele Dinge können die Luftzirkulation behindern, wie z.B. unordentlich verlegte Flachbandkabel (die ältere Speichergeräte verwenden), zu viele in einem winzigen Gehäuse gedrängt untergebrachte Laufwerke, Lüfter, die von Staub oder Tierhaaren gebremst werden, usw.

Techniker müssen sich dieser Gefahren beim Hinzufügen einer neuen Festplatte in einem alten System bewusst sein. Machen Sie es sich zur Gewohnheit, Flachbandkabel möglichst zu befestigen, Lüfter an der Gehäusevorderseite einzubauen, wenn die Systeme gelegentlich und unvermittelt abstürzen, und achten Sie darauf, dass die Lüfter auch wirklich laufen. Und wenn schließlich ein Kunde ein neues Laufwerk haben möchte, sein System aber in einem winzigen Minitower steckt, der nur über den Lüfter des Netzteils gekühlt wird, dann empfehlen Sie ihm höflich, aber bestimmt eines der langsameren Laufwerke!

Formfaktoren

Magnetische Festplatten werden in zwei standardisierten Größen hergestellt, nämlich 2,5 und 3,5 Zoll (Abbildung 8.4). Desktop-Systeme können beide Formfaktoren verwenden, die meisten Laptops verwenden 2,5-Zoll-Laufwerke. Der Formfaktor legt lediglich die Größe fest. Die Anschlüsse und Speichertechnologien der Laufwerke können sich unterscheiden.



Abb. 8.4: 2,5-Zoll-Laufwerk auf einem 3,5-Zoll-Laufwerk

8.1.2 Solid-State Drives (SSDs)

Das Starten eines Rechners dauert, weil herkömmliche Festplatten erst einmal hochdrehen und die Schreib/Leseköpfe die Daten vom Laufwerk in den Arbeitsspeicher einlesen müssen. Für alle beweglichen Metallteile der auf Platten basierenden Laufwerke wird eine Menge Energie benötigt. Sie produzieren viel Wärme, benötigen einiges an Platz, verschleißen mit der Zeit und brauchen eine Menge Nanosekunden zur Erledigung ihrer Aufgaben. Bei *Halbleiterlaufwerken*, die meist *Solid-State Drive* (*SSD*) oder auch *Solid-State-Laufwerk* genannt werden, entfallen die meisten dieser Probleme.

Technisch gesehen handelt es sich bei der Solid-State-Technologie und den entsprechenden Geräten um eine Kombination aus Halbleitern und Transistoren, aus denen elektrische Komponenten ohne bewegliche Teile erstellt werden. Das sind einige seltsame Begriffe, die ich nun näher erläutern werde.

Einfach ausgedrückt verwenden SSDs (Abbildung 8.5) zum Speichern der Daten Speicherchips anstelle dieser verflixten mechanischen Bauteile, die bei herkömmlichen Festplatten verwendet werden.



Abb. 8.5: Ein Solid-State-Laufwerk

Die Solid-State-Technologie wird verbreitet für Desktop- und Laptop-Festplattenlaufwerke, Speicherkarten, Kameras, USB-Sticks und andere kleine elektronische Geräte verwendet.

SSDs für PCs sind in drei Größen erhältlich: im eben erwähnten 2,5-Zoll-Formfaktor und als zwei flachere Formfaktoren, die mSATA und M.2 heißen (Abbildung 8.6), mSATA- und M.2-SSDs werden in speziellen Steckplätzen auf dem Mainboard installiert (Abbildung 8.7). Viele aktuelle Mainboards besitzen zwei oder mehr M.2-Steckplätze.



Abb. 8.6: M.2-SSD

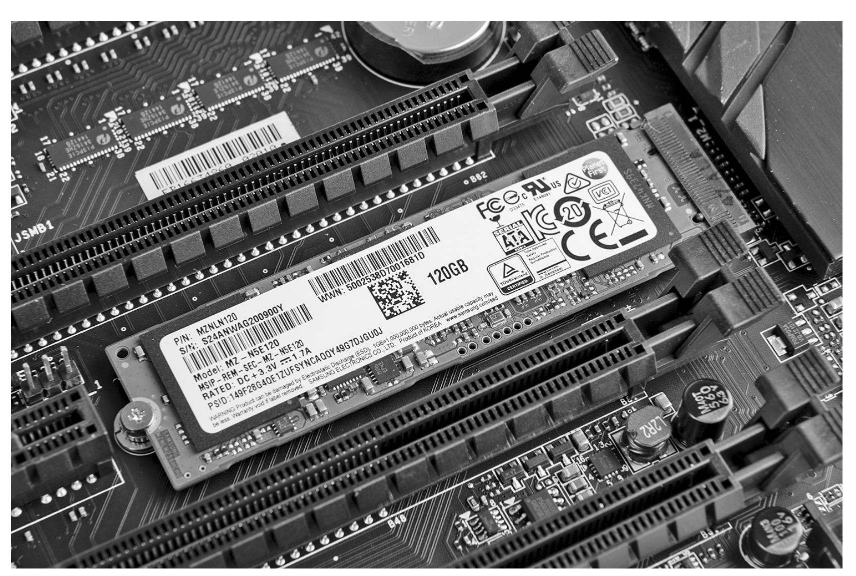


Abb. 8.7: Auf einem Mainboard installierte M.2-SSD

Wichtig

mSATA-Karten sind zwar noch erhältlich, die Technologie wird aber zweifelsohne sowohl bei Desktops als auch bei Laptops von M.2 abgelöst werden. M.2-Laufwerke sind nur halb so groß und bieten eine deutlich bessere Leistung. Im Lernziel 3.4 der CompTIA A+-Prüfung 1001 ist irrtümlich von M2 (ohne Punkt) die Rede.

Es gibt eine Vielzahl unterschiedlicher M.2-Steckplätze, die für verschiedene Arten der Verwendung als Massenspeicher gekennzeichnet sind. Als Schlüssel werden Buchstaben benutzt. Mit dem Schlüssel B, M oder B+M gekennzeichnete M.2-Steckplätze unterstützen beispielsweise Massenspeichergeräte. Andere Steckplätze, wie die mit dem Schlüssel A oder F, werden in drahtlosen Netzwerkgeräten verwendet. Die Spezifikationen der Schlüssel gehen über die aktuelle A+-Prüfung hinaus, aber es sieht so aus, als sei M.2 gekommen, um zu bleiben, deshalb sollten Sie die Varianten kennen.

Heutzutage verwenden SSDs nichtflüchtigen Flash-Speicher (z.B. NAND) und behalten die Daten auch nach dem Abschalten oder dem Trennen vom Gerät. (Mehr über die Flash-Speichertechnologie erfahren Sie in Kapitel 10, *Eingabe/Ausgabe*.)

Kosten

SSDs sind teurer als herkömmliche Festplattenlaufwerke. Bei preiswerteren SSDs werden typischerweise weniger zuverlässige MLC-Speichertechnologien (Multi-Level Cell) anstelle der effizienteren SLC-Technologie (Single-Level Cell) verwendet, um Kosten zu senken. Die bei SSDs verbreitetste Speichertechnologie ist 3D-NAND, eine MLC-Variante, bei der die Speicherzellen übereinandergestapelt werden, um höhere Speicherdichten und damit auch höhere Speicherkapazitäten zu erzielen.

SSDs verteilen die Daten beim Speichern entsprechend den Vorgaben des SSD-Controllers wahllos nach dem Gießkannenprinzip auf Hochgeschwindigkeitsspeicherzellen. Dieser Vorgang bleibt dem Betriebssystem allerdings verborgen, dem die SSD eine elektronische Fassade präsentiert und als herkömmliches Laufwerk erscheint.

Leistungskennzahlen

Beim Kauf einer SSD sind drei Kriterien zu beachten: Wie schnell kann sie lange Datensequenzen lesen oder schreiben, die im gleichen Bereich des Laufwerks gespeichert werden? Wie schnell kann sie kleine Datenblöcke lesen oder schreiben, die zufällig auf dem Laufwerk verteilt sind? Und wie schnell reagiert sie auf eine einzelne Anfrage (Latenz)? Wie wichtig die jeweiligen Kennzahlen sind, hängt davon ab, wofür Sie das Laufwerk einsetzen möchten. Bevor wir uns damit befassen, wie die Leistungskennzahlen zu beurteilen sind, betrachten wir zunächst einmal, wie die Hersteller die Leistung beim Lesen/Schreiben sequenzieller Daten, zufällig verteilter Daten und die Latenz messen.

Leistung beim sequenziellen Lesen/Schreiben Ein gängiges Maß für die Geschwindigkeit eines Speichergeräts ist der Datendurchsatz, also die Datenrate, mit der lange Datensequenzen gelesen oder geschrieben werden können. Der Datendurchsatz bei sequenziellem Lesen/Schreiben wird üblicherweise in Megabyte pro Sekunde (MBps) angegeben. Die meisten Laufwerke können ein wenig schneller lesen als schreiben.

Zum Vergleich: Herkömmliche Festplatten erreichen einen Datendurchsatz, der 200 MBps nicht übertrifft; SATA-SSDs schaffen 600 MBps und NVMe-SSDs erzielen sogar 2500 MBps oder mehr. Diese Zahlen sind nützlich, wenn absehbar ist, dass Ihre Laufwerke häufig sehr große Dateien lesen und schreiben sollen, in der Praxis ist das jedoch eher selten.

Leistung beim zufälligen Lesen/Schreiben Da Laufwerke in der Praxis nur selten ständig sehr große Dateien lesen oder schreiben, werfen wir auch einen Blick auf die Leistung, die ein Laufwerk erreicht, wenn es zufällig verteilte Daten lesen, schreiben oder lesen und schreiben (Mischbetrieb) muss. Wir messen also, wie oft ein kleiner Datenblock fester Größe, der an einer zufälligen Stelle auf dem Laufwerk gespeichert ist, pro Sekunde gelesen oder geschrieben werden kann.

Bei diesen Messwerten wird meistens die Größe des Datenblocks angegeben, deshalb werden sie als *4K Lesen*, *4K zufälliges Schreiben*, *4K Lesen/Schreiben* usw. bezeichnet. Für gewöhnlich wird die Anzahl der Ein/Ausgabeoperationen pro Sekunde (*Input/Output Operations Per Second*, IOPS) angegeben, manchmal aber auch ein MBps-Wert. Herkömmliche Festplatten erreichen weniger als 150 IOPS, die neuesten NVMe-SSDs hingegen schaffen *mehrere Hunderttausend* IOPS.

Latenz Es ist ebenfalls sinnvoll, die *Reaktionszeit*, *Zugriffszeit* oder *Latenz* eines Laufwerks unter die Lupe zu nehmen, die angibt, wie schnell es auf eine einzelne Anfrage reagiert. Die Latenz wird üblicherweise in Millisekunden (ms) oder Mikrosekunden (µs) angegeben.Für Hochleistungsdatei- oder Datenbankserver ist Speicher mit niedriger Latenz unverzichtbar, aber die Latenz der meisten modernen Laufwerke ist für den allgemeinen Gebrauch ausreichend. Zum Vergleich: Herkömmliche Festplatten erreichen eine Latenz von knapp 20 ms, SSDs dagegen erzielen Latenzen, die deutlich unter einer Millisekunde liegen.

Welche Kombination aus Leistung und Preis in einer bestimmten Situation sinnvoll ist, hängt von vielen Faktoren ab. Ein typischer Rechner lastet eine SSD beispielsweise kaum aus. Der Benutzer startet den Rechner, öffnet ein oder zwei Anwendungen und arbeitet vor sich hin. Für die zum Booten oder zum Start von Anwendungen benötigte Zeit spielt die Qualität der SSD eine Rolle, aber danach wird der Rechner kaum ins Schwitzen kommen. Eine Workstation zur Bearbeitung hochwertiger Videos hingegen könnte stundenlang riesige Dateien lesen und schreiben. Und ein großer Dateiserver muss möglicherweise in jeder Minute Tausende kleiner Dateien lesen und schreiben.

Das bedeutet in der Praxis, dass eine preiswertere, weniger leistungsstarke SSD für einen Computer, mit dem allgemeine Arbeiten erledigt werden, ausreicht. Stehen anspruchsvollere Aufgaben an, muss man etwas mehr Geld für eine leistungsfähigere SSD ausgeben. Wenn es darum geht, eine bestimmte leistungsstarke SSD auszuwählen, können die Kriterien Datendurchsatz, IOPS und Latenz verhindern, dass Sie zu viel Geld für Leistungsmerkmale ausgeben, die für Ihren Anwendungsfall gar keine Rolle spielen.

8.1.3 Hybridlaufwerke

Windows unterstützt *Hybridlaufwerke* (*HHDs – Hybrid Hard Drives* oder auch *SSHDs*). Dabei handelt es sich um Laufwerke, die Flash-Speicher und herkömmliche plattenbasierte Laufwerke kombinieren, um schnellen und zuverlässigen Speicher bereitzustellen. Die kleine SSD in diesen Laufwerken ermöglicht es, die Daten, auf die am häufigsten zugegriffen wird, im Flash-Speicher abzulegen, um beispielsweise die Startzeit zu verkürzen. Und weil die Platten nicht so oft hochdrehen müssen, verlängert sich bei tragbaren Computern auch die Akkulaufzeit.

Computer von Apple verwenden ein sogenanntes *Fusion Drive*, das auf dem gleichen Konzept beruht wie Hybridlaufwerke. Das Fusion Drive besteht aus einer normalen Festplatte und einer SSD. macOS entscheidet automatisch, welche Daten auf der SSD gespeichert werden.

8.2 Anschließen von Massenspeichergeräten

Für die Kommunikation von CPU und einem Massenspeichergerät müssen zwei Voraussetzungen erfüllt sein. Zum einen muss es eine standardisierte physische Verbindung zwischen CPU, Laufwerk-Controller und dem Laufwerk geben. Diese Verbindung muss die Daten so schnell wie möglich zwischen diesen Geräten übertragen, ohne dass es dabei zu Übermittlungsfehlern kommt (Abbildung 8.8).

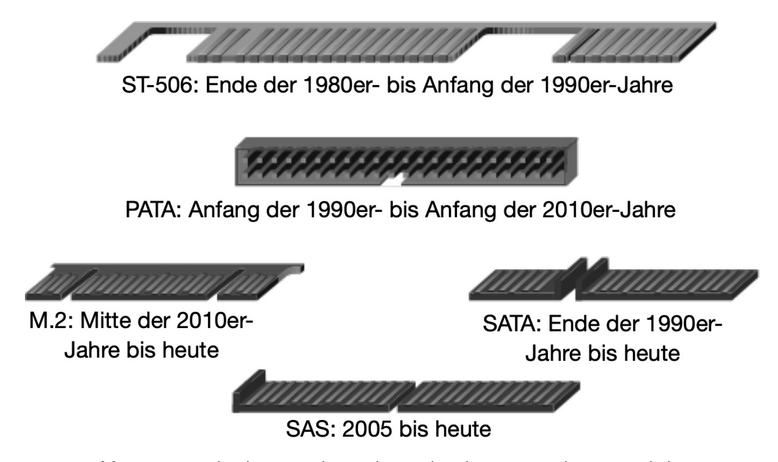


Abb. 8.8: Standardisierte physische Verbindungen sind unverzichtbar.

Zum anderen muss die CPU ein standardisiertes Protokoll verwenden, wie eine spezielle Sprache, damit sie den Massenspeichergeräten mitteilen kann, Daten zu lesen oder zu scheiben (Abbildung 8.9).

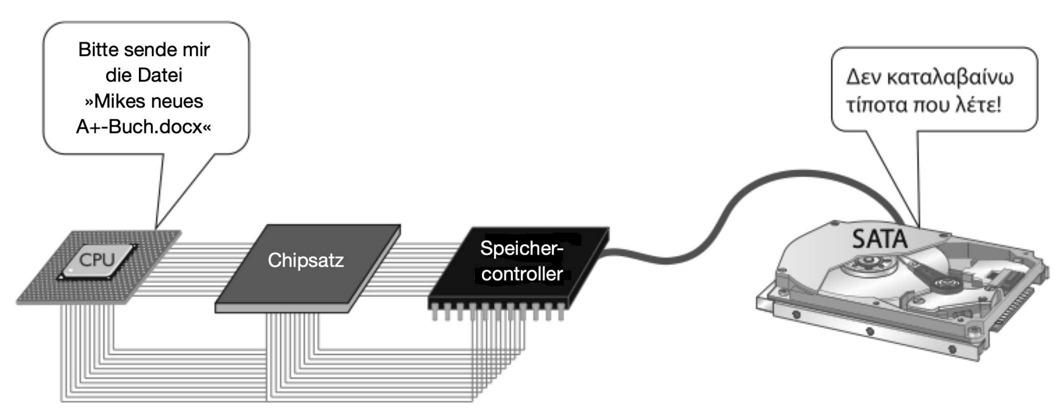


Abb. 8.9: Wir brauchen eine gemeinsame Sprache!

In den meisten Fällen ist es ein und dieselbe Organisation, die sowohl die physischen Verbindungen als auch die zur Kommunikation verwendete Sprache definiert. Seit mehr als 25 Jahren definiert das Small Form Factor (SFF) Committee der Storage Networking Industry Association die Standards für Massenspeicher, wobei diejenigen für ATA/ATAPI für CompTIA A+-Techniker am wichtigsten sind.

Hinweis

Besuchen Sie die Website `https://www.snia.org`. Dort finden Sie viele Informationen über die Standards von Massenspeichern.

Etwa 1990 erschien Version 1 einer neuen Schnittstellentechnik namens *ATA* (*Advanced Technology Attachment*), die bis zur ATA/ATAPI-Version 7 weiterentwickelt wurde. Für Techniker sind nur zwei Versionen dieses Standards von Interesse: PATA und SATA. Parallel ATA (PATA) wurde mit der ATA/ATAPI-Version 1 eingeführt. Serial ATA (SATA) erschien zusammen mit der ATA/ATAPI-Version 7. Sehen wir uns die beiden Standards an.

Hinweis

ATA-Festplatten werden oft als *IDE*-Laufwerke (*Integrated Drive Electronics*) bezeichnet. Der Begriff bezieht sich auf jedes Festplattenlaufwerk mit eingebautem Controller. Technisch gesehen handelt es sich bei allen Festplatten um IDE-Laufwerke, obwohl wir den Begriff IDE nur im Zusammenhang mit PATA-Laufwerken verwenden.

8.2.1 PATA

PATA-Laufwerke sind leicht an ihren Daten- und Stromanschlüssen zu erkennen. Sie verwenden ein 40-adriges Flachbandkabel, das normalerweise direkt am Mainboard angeschlossen wird. Beachten Sie, dass diese Kabel in der Prüfung als IDE-Kabel bezeichnet werden. Abbildung 8.10 zeigt ein Beispiel für eine solche Verbindung. Alle PATA-Laufwerke verwenden den Standard-Molex-Stecker zur Stromversorgung (Abbildung 8.11).



Abb. 8.10: Am Mainboard angeschlossenes PATA-Kabel



Abb. 8.11: Molex-Stecker und Molex-Buchse (rechts) einer PATA-Festplatte

Hinweis

Der letzte ATA/ATAPI-Standard, der PATA erwähnt, unterstützte sehr große Laufwerke (144 Petabyte (PB), mehr als 144 Millionen GB) mit Datenübertragungsraten von bis zu 133 Megabyte pro Sekunde (MBps). Über ein PATA-Flachbandkabel konnten an einen einzigen ATA-Controller bis zu zwei PATA-Laufwerke angeschlossen werden, also Festplatten, optische Laufwerke oder Bandlaufwerke. Mittels Steckbrücken (Jumper) wurde eines der Laufwerke als *Master* und das andere als *Slave* konfiguriert. (Mehr dazu später, wenn es um die Installation geht.)

Der ATA-Standard wurde sieben Mal grundlegend überarbeitet, wobei jedes Mal eine Erhöhung der Geschwindigkeit und/oder der Speicherkapazität stattfand. Ich könnte an dieser Stelle leicht 15 Seiten mit sämtlichen Änderungen füllen, aber als heutiger Techniker brauchen Sie all diese Einzelheiten nicht zu wissen. Eins der Features existiert aber auch heute noch, nämlich S.M.A.R.T.

Mit der ATA/ATAPI-Version 3 wurde *S.M.A.R.T.* (*Self-Monitoring Analysis and Reporting Technologies*) eingeführt, ein internes Programm, das durch Überwachung der mechanischen Komponenten und Laufwerksfehler dabei hilft, Ausfälle von Festplattenlaufwerken vorherzusagen. Die Informationen werden in nichtflüchtigem Speicher abgelegt und können mit einer speziellen Software ausgelesen werden. Es gibt allgemein funktionsfähige Programme zum Auslesen der S.M.A.R.T.-Daten und jeder Laufwerkshersteller bietet eigene Software zum Abrufen herstellerspezifischer Informationen an. Regelmäßige Verwendung der S.M.A.R.T.-Software hilft Ihnen dabei, die Funktionalität Ihrer Festplatten zu überprüfen und mögliche Ausfälle vorherzusagen.

8.2.2 SATA

Trotz seiner Langlebigkeit als vorrangige Massenspeicherschnittstelle beim PC war PATA nicht frei von Problemen. Erstens behinderten die Flachbandkabel die Luftzirkulation und es war zuweilen eine Qual, sie ordentlich zu verlegen. Zweitens durften die Kabel höchstens 45 Zentimeter lang sein. Drittens ließen sich PATA-Laufwerke nicht im laufenden Betrieb wechseln (*Hot-Swapping*). Sie mussten das System erst vollständig herunterfahren, bevor Sie ein Laufwerk installieren oder austauschen konnten. Und schließlich hatte die Technologie hinsichtlich der Datenrate ihre Grenzen erreicht. Es wurde Zeit, die Verbindung und das Protokoll für ATA/ATAPI-Laufwerke umzugestalten.

SATA beseitigte diese Probleme. SATA arbeitet mit Punkt-zu-Punkt-Verbindungen zwischen den SATA-Geräten (Festplatten, SSDs, optische Laufwerke usw.) und dem SATA-Controller, der auch *HBA* (*Host Bus Adapter*) genannt wird. Auf den ersten Blick sehen SATA-Geräte genau wie PATA-Standardgeräte aus. Die Anschlüsse für Daten- und Stromkabel unterscheiden sich aber wesentlich (Abbildung 8.12).



Abb. 8.12: Stromkabel (links) und Stecker (rechts) einer SATA-Festplatte

Da SATA-Geräte die Daten seriell und nicht parallel übertragen, kommt die SATA-Schnittstelle mit weit weniger physischen Leitungen aus (sieben anstelle der für PATA typischen 40 Leitungen), sodass viel dünnere Kabel verwendet werden können. Das dünnere Kabel sorgt für eine bessere Luftzirkulation im PC-Gehäuse und lässt sich leichter verlegen, was die Kühlung verbessert.

Zudem darf das Kabel bei SATA-Geräten mehr als doppelt so lang wie bei PATA-Geräten sein (ein Meter statt 45 cm). Das erleichtert die Installation in größeren Gehäusen.

Wichtig

In den Lernzielen der CompTIA A+-Prüfung 1001 wird das 40-adrige PATA-Flachbandkabel als DIE-Kabel bezeichnet. Damit ist das Gleiche gemeint.

SATA hat das ganze Master/Slave-Konzept abgeschafft. Jedes Laufwerk wird mit einem eigenen Anschluss verbunden und es werden keine Laufwerke mehr hintereinander geschaltet. Darüber hinaus gibt es keine Beschränkung hinsichtlich der Anzahl der Laufwerke. Viele Mainboards unterstützen bis zu acht SATA-Laufwerke (Abbildung 8.13), und wenn Sie mehr brauchen, dann setzen Sie eine Steckkarte mit SATA-HBA in den Rechner ein und schließen Ihre Laufwerke daran an!

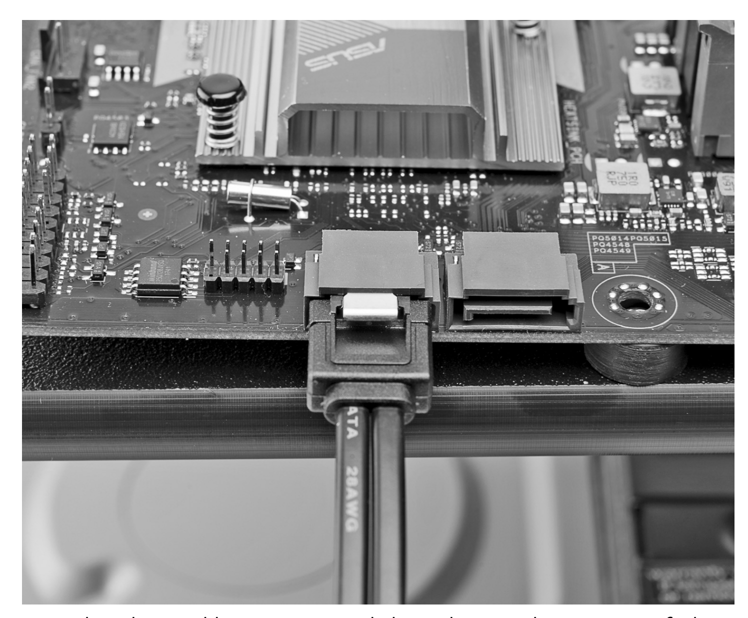


Abb. 8.13: Am Mainboard angeschlossenes SATA-Kabel. Beachten Sie den zweiten verfügbaren Anschluss.

Das Beste ist jedoch der Datendurchsatz. Wie der Name schon sagt, übertragen SATA-Laufwerke die Daten seriell und nicht mehr parallel, wie es bei PATA-Laufwerken der Fall war. Man sollte zwar glauben, dass serielle Geräte eigentlich nicht schneller als parallele Geräte sein können, aber das ist falsch. Einzelne Datenströme wie bei SATA-Geräten lassen sich sehr viel schneller übertragen als mehrere parallele Datenströme (wie bei parallelen IDE-Geräten) und zwar theoretisch bis zu 30-mal schneller. SATA-Laufwerke gibt es in drei gängigen Varianten (1,5 Gbps, 3 Gbps und 6 Gbps) mit einem maximalen Durchsatz von 150, 300 bzw. 600 MBps. Falls ein System über einen eSATA-Anschluss verfügt, verwendet dieser dieselbe Variante und Geschwindigkeit wie der interne SATA-Anschluss.

Viele verschiedene Gerätetypen an ein voll funktionsfähiges und laufendes System anzuschließen, kann zu einer Katastrophe führen. Möglicherweise wird ein Gerät einfach nur nicht erkannt, es kann aber schlimmstenfalls auch zu einer Beschädigung des Geräts oder des Computers kommen. Mittlerweile lassen sich die Geräte jedoch im laufenden Betrieb austauschen. Das Hot-Swapping setzt zwei Dinge voraus. Erstens muss es möglich sein, ein Laufwerk im laufenden Betrieb am Computer anzuschließen, ohne dass eines der Geräte dabei Schaden nimmt. Zweitens muss das Laufwerk automatisch erkannt und voll funktionsfähig in das System eingebunden werden, sobald es angeschlossen ist. Bei SATA funktioniert das Hot-Swapping problemlos (siehe dazu den Abschnitt *AHCI* später in diesem Kapitel).

Hinweis

Leser, die sich mit den Zahlen auskennen, haben vielleicht die Diskrepanz zwischen den Namen und den Durchsätzen der beiden SATA-Varianten bemerkt. Schließlich ergibt sich aus den 1,5 Gbps von SATA 1.0 mit 192 MBps eine deutlich höhere als die angegebene Geschwindigkeit von »nur« 150 MBps. Die bei

SATA-Laufwerken verwendete Datencodierung belegt etwa 20 Prozent der Bandbreite durch Verwaltungsdaten, womit 80 Prozent für die reine Datenbandbreite übrig bleiben.

Die 3-Gbps-Variante (SATA 2.0) hat für allerlei Probleme gesorgt, weil der für die Spezifikationen verantwortliche Ausschuss SATA-II-Ausschuss genannt wurde und diese Bezeichnung für Marketingzwecke aufgegriffen wurde. Deshalb ist oft auch von SATA-II-Laufwerken und nicht von 3-Gbps-Laufwerken die Rede.

Der SATA-Ausschuss trägt heute den Namen SATA-IO. Als die SATA-II-Geschwindigkeit auf 6 Gbps verdoppelt wurde, gab es dementsprechend ebenfalls zwei Bezeichnungen: SATA-III und SATA 6 Gbps.

SATA Express (SATAe) oder SATA 3.2, bindet kompatible Laufwerke direkt am PCI-Express-Bus des Mainboards ein. SATAe verzichtet auf die Link- und Transportebene, um die volle Leistungsfähigkeit von PCIe auszuschöpfen. Durch den Verzicht auf diesen Verwaltungsaufwand erhöht sich der Datendurchsatz von SATA enorm: Jede PCI-3.0-Lane erreicht eine Datenübertragungsrate von bis zu 8 Gbps. Ein Laufwerk, das zwei Lanes nutzt, erzielt somit auf dem Bus eine Datenübertragungsrate von satten 16 Gbps. Ohne den Verwaltungsaufwand früherer SATA-Versionen ergeben sich somit 2000 MBps!

SATAe nutzt einen eigenen Anschluss, ist aber abwärtskompatibel zu früheren SATA-Versionen (Abbildung 8.14). Beachten Sie, dass der mittlere und der linke Teil der Buchse genauso aussehen wie normale SATA-Anschlüsse. Und so funktionieren sie auch. Sie können an einem SATAe-Anschluss zwei normale SATA-Laufwerke anschließen. Sie können Ihr Mainboard also bedenkenlos aufrüsten! Natürlich muss Ihr Mainboard SATAe auch unterstützen, damit Sie in den Genuss dieser extrem schnellen SATA-Laufwerke kommen können.

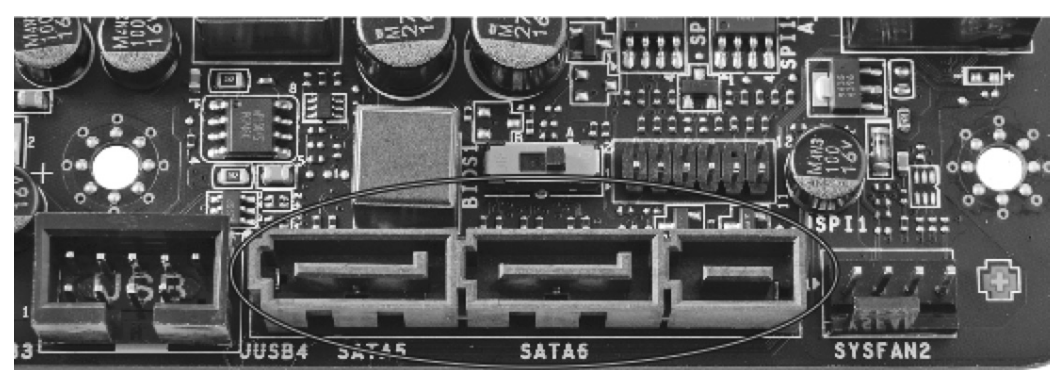


Abb. 8.14: SATAe-Anschluss

Wichtig

Mit Ausnahme von SATAe ist jede der SATA-Varianten nach der entsprechenden Überarbeitung der SATA-Spezifikationen benannt, in der die Verbesserungen vorgestellt wurden:

SATA 1.0: 1,5 Gbps/150 MBps

SATA 2.0: 3 Gbps/300 MBps

SATA 3.0: 6 Gbps/600 MBps

SATA 3.2: bis zu 16 Gbps/2000 MBps, auch als SATAe bezeichnet

Der problemlose Umgang mit SATA hat es zur ersten Wahl als Massenspeicher bei Desktop-Systemen gemacht. Die meisten aller heute verkauften Festplatten sind SATA-Laufwerke.

Hinweis

Die 2016 überarbeitete Version SATA 3.3 erhöht unter anderem die Größe der unterstützten Laufwerke. Der Datendurchsatz der Schnittstelle wurde aber nicht erhöht.

eSATA und andere externe Laufwerke

Wie der Name bereits besagt, erweitert *eSATA* (*External SATA*) den SATA-Bus auf externe Geräte. Die eSATA-Laufwerke verwenden ähnliche Stecker wie internes SATA, die jedoch anders geformt sind, damit Sie diese nicht verwechseln können. Abbildung 8.15 zeigt einen eSATA-Anschluss an der Rückseite eines Mainboards.

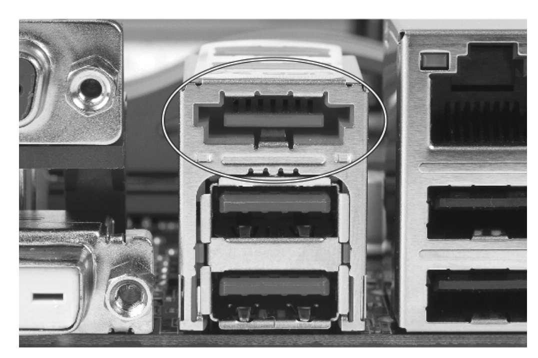


Abb. 8.15: eSATA-Anschluss

eSATA verwendete abgeschirmte Kabel von bis zu zwei Meter Länge außerhalb des PCs und unterstützt Hot-Swapping. eSATA erweiterte den SATA-Buss, dessen volle Geschwindigkeit die der schnellsten USB-Verbindung leicht übertraf.

Als USB 3.0 auf den Markt kam, erlebte eSATA einen Niedergang und war schnell verschwunden. Sie finden es heute nur noch in sehr alten Systemen und Festplattengehäusen – und in der CompTIA A+-Prüfung.

Wichtig

In den Lernzielen der CompTIA A+-Prüfung 1001 werden eSATA-Steckkarten erwähnt, die in Systeme eingebaut werden können, die nicht über diesen Anschluss verfügen. Sie können diese Karten heute noch kaufen, um ältere externe Massenspeichergeräte zu unterstützen.

Heutige externe HDD- und SSDs-Gehäuse verwenden USB- (3.0, 3.1 oder C) oder Thunderbolt-Anschlüsse. In Kapitel 10 werden die Unterschiede zwischen diesen Anschlüssen erläutert. Die Laufwerke in diesen Gehäusen sind Standard-HDDs oder -SSDs.

Wichtig

Sie sollten die erlaubte Kabellänge der verschiedenen Anschlüsse kennen:

SATA: 1 Meter

eSATA: 2 Meter

PATA: 45 Zentimeter

8.2.3 Kommunikation mit Massenspeichergeräten

Der ursprüngliche ATA-Standard definierte einen speziellen Befehlssatz für die CPU, um mit dem Laufwerk-Controller zu kommunizieren. Die aktuellen Befehlssätze heißen AHCI und NVMe. Es gibt auch noch den SCSI-Befehlssatz, allerdings vornehmlich auf dem Servermarkt.

AHCI

Aktuelle Windows-Versionen unterstützen mit *AHCI* (*Advanced Host Controller Interface*) ein effizientes Verfahren im Zusammenspiel mit SATA-HBAs. Bei Verwendung von AHCI werden einige der anspruchsvolleren SATA-Funktionen verfügbar, wie z.B. Hot-Swapping und native Befehlswarteschlangen.

Bei *NCQ* (*Native Command Queuing*) bzw. der *nativen Befehlswarteschlange* handelt es sich um eine Optimierungsfunktion von SATA-Laufwerken, durch die höhere Lese- und Schreibgeschwindigkeiten erzielt werden, die mit den alten PATA-Laufwerken schlicht und einfach nicht möglich sind. SATA unterstützt Hot-Swapping, allerdings müssen Mainboard und Betriebssystem dies ebenfalls unterstützen.

AHCI wird auf der CMOS-Ebene implementiert (siehe Abschnitt 8.5, *BIOS-Unterstützung: CMOS-Einstellungen und Treiberinstallation*) und muss generell vor der Installation des Betriebssystems aktiviert werden. Wenn Sie es erst nach der Installation aktivieren, dann zeigt Windows den berüchtigten blauen Bildschirm an. Wie nett.

Hinweis: Wechseln des SATA-Modus ohne Neuinstallation

Sie können versuchen, AHCI in Windows zu aktivieren, ohne eine Neuinstallation durchführen zu müssen. Das könnte beispielsweise notwendig sein, wenn ein Kunde Windows versehentlich im veralteten IDI-Modus installiert hat und dann feststellt, dass seine neue SSD AHCI benötigt, um vernünftig zu funktionieren.

Erstellen Sie zunächst ein Backup, bevor Sie versuchen, die Aktivierung vorzunehmen. Zudem müssen Sie einige Schritte in Windows ausführen, bevor Sie die BIOS/UEFI-Einstellung ändern. In Windows 7 und 8/8.1 müssen manuelle Änderungen an der Registry vorgenommen werden (siehe Kapitel 12, *Windows unter der Haube*). Windows 10 verwendet eine Eingabeaufforderung mit Administratorrechten (siehe Kapitel 15, *Eingabeaufforderung*).

Eine kurze Recherche im Internet (Stichwörter »IDI, AHCI, Windows«) fördert viele ausgezeichnete schrittweise Anleitungen für Windows 7/8/8.1 und Windows 10 zutage. Aber denken Sie an das Backup!

Wenn Sie ein SATA-Laufwerk an einen laufenden Windows-Computer anschließen, auf dem AHCI nicht aktiviert ist, wird es auch nicht automatisch angezeigt. Ist AHCI hingegen aktiviert, sollte es augenblicklich erscheinen, wie man es von einem Hot-Swapping-fähigen Gerät erwartet.

NVMe

AHCI ist dafür ausgelegt, die Lesegeschwindigkeit plattenbasierter SATA-Laufwerke zu optimieren und einen Austausch im laufenden Betrieb zu gestatten. Als Konfigurationseinstellung funktioniert es auch mit vielen SSDs, ist aber keine ideale Lösung. Das liegt daran, dass SSDs zur Zusammenarbeit mit dem Betriebssystem Schaltkreise besitzen, die sie dem Betriebssystem als herkömmliche, plattenbasierte Laufwerke erscheinen lassen. Wenn eine Schreib/Leseoperation erfolgt, übersetzt das virtuelle SSD-Laufwerk die Anfrage in eine Speicheradresse, auf die es zugreifen kann.

Die *NVMe*-Spezifikation (*Non-Volatile Memory Express*) ermöglicht die direkte Kommunikation zwischen Betriebssystem und SSD über eine Lane des PCIe-Busses, wodurch die Latenzzeit verringert und die enorme Geschwindigkeit von High-End-SSDs voll ausgeschöpft wird (Abbildung 8.16). NVMe-SSDs sind in verschieden Formfaktoren erhältlich, etwa als Erweiterungskarten oder insbesondere im M.2-Format. NVMe-SSDs sind derzeit noch erheblich teurer als andere SSDs, bieten aber auch eine viel höhere Geschwindigkeit. NVMe-Laufwerke verwenden SATAe.

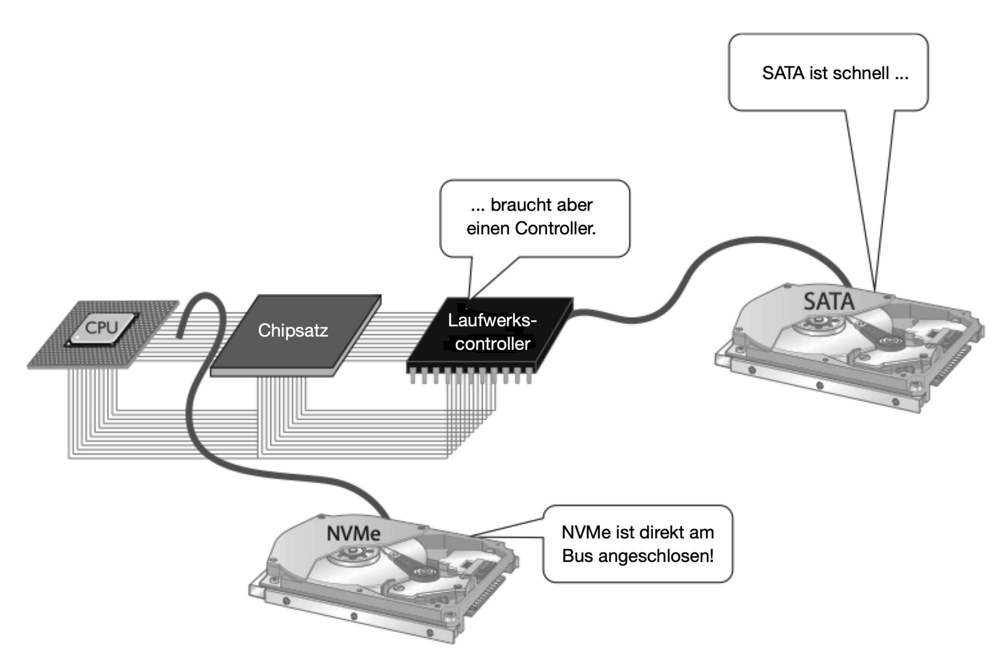


Abb. 8.16: NVMe kommuniziert direkt über den Bus

SCSI

SATA-Laufwerke dominieren den PC-Markt, aber eine weitere Laufwerkstechnologie namens *Small Computer System Interface* (SCSI) beherrscht den Servermarkt. SCSI gibt es, seit die ersten HDDs auf den Markt kamen, und hat sich im Lauf der Jahre von einer parallelen und breiteren parallelen zu verschiedenen superschnellen – das sollte inzwischen klar sein – seriellen Schnittstellen weiterentwickelt. SCSI-Geräte – parallele und serielle – verwenden einen standardisierten SCSI-Befehlssatz, sodass an ein System alte und neue Geräte angeschlossen werden können, die problemlos miteinander kommunizieren. SCSI-Laufwerke verwenden eine Vielzahl verschiedener Flachbandkabel, die sich von Version zu Version unterscheiden.

Laufwerke mit *Serial Attached SCSI* (SAS) dienen als schneller und robuster Speicher für Server und Speicher-Arrays. Die neueste SAS-Schnittstelle SAS-3 bietet Geschwindigkeiten von bis zu 12 Gbps. SAS-Controller unterstützen auch SATA-Laufwerke, was Technikern erfreulicherweise eine große Flexibilität ermöglicht, insbesondere dann, wenn man es mit kleineren Serversystemen zu tun hat. Für SAS-Implementierungen gibt es mehr als ein Dutzend verschiedene Steckertypen. Die meisten davon sehen wie eine etwas klobigere Version eines SATA-Steckers aus.

In der CompTIA A+-Zertifizierung kommt SCSI vor, aber damit ist wohl nur SAS gemeint. Wenn Sie sich zum Servertechniker fortbilden möchten, müssen Sie SCSI allerdings unbedingt kennen. Die Website der SCSI Trade Asociation (STA) ist ein guter Ausgangspunkt: `https://www.scsita.org`.

8.3 Datensicherheit mit RAID

Wenn Sie erfahrene Techniker nach dem wertvollsten Bestandteil eines PCs fragen, dann werden Ihnen alle antworten: die Daten. Für ein paar Hunderter können Sie jede PC-Komponente austauschen. Wenn Sie aber kritische Daten verlieren ... Nun, lassen Sie es mich so ausdrücken: Mir sind zwei kleine Unternehmen bekannt, deren Ende durch den Verlust jeweils einer Festplatte mit Daten besiegelt war.

Die Daten sind enorm wichtig. Daten stellen die Daseinsberechtigung für Ihren PC dar; ohne Daten bräuchten Sie auch keinen Computer. Datenverluste können schlimme Folgen haben. Daher brau-

chen wir Verfahren, um Datenverluste zu vermeiden. Natürlich können Sie Daten sichern, aber wenn eine Festplatte ausfällt, dann müssen Sie den Rechner herunterfahren, eine neue Festplatte installieren, das Betriebssystem neu installieren und dann die Sicherung wiederherstellen. Daran ist nichts falsch, sofern Sie sich die Ausfallzeiten leisten und vorübergehend auch ohne Rechner auskommen können.

Eine bessere Lösung wäre natürlich, wenn Ihre Daten selbst dann erhalten bleiben, wenn eine Festplatte ausfällt, damit Sie weiterarbeiten können. Das ist allerdings nur dann möglich, wenn Sie sich nicht mehr nur auf eine einzige Festplatte verlassen und zwei oder mehr zur Speicherung der Daten verwenden. Klingt zwar gut, aber wie lässt sich dies erreichen? Zunächst einmal können Sie natürlich einen Festplatten-Controller installieren, der die Daten gleichzeitig auf zwei Festplatten schreibt (Abbildung 8.17). Dabei sind die Daten auf beiden Laufwerken immer identisch. Ein Laufwerk wäre dabei das primäre und eines das gespiegelte Laufwerk, das erst dann wirklich genutzt wird, wenn das primäre Laufwerk ausfällt. Dieses Verfahren, bei dem die Daten gleichzeitig auf zwei Festplatten geschrieben werden, wird *Disk Mirroring* bzw. *Festplattenspiegelung* genannt.

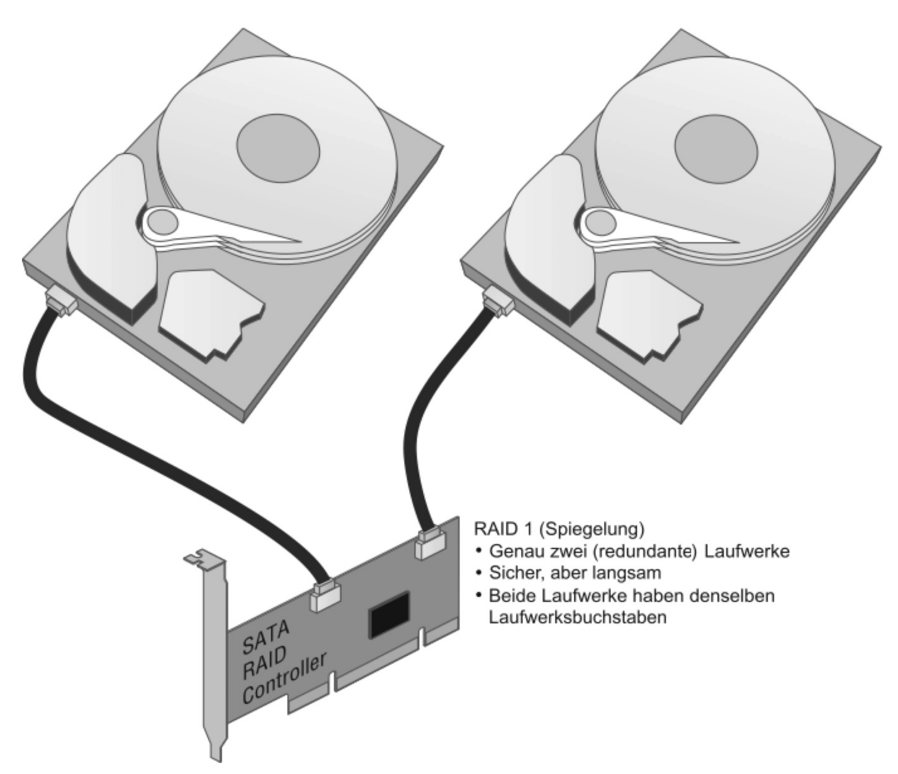


Abb. 8.17: Festplattenspiegelung

Noch ein wenig mehr Sicherheit bieten Systeme mit zwei getrennten Controllern für die Laufwerke. Wenn zwei Laufwerke an getrennte Controller angeschlossen werden, dann arbeitet das System auch dann noch weiter, wenn der Controller des primären Laufwerks ausfällt. Diese anspruchsvolle Variante der Spiegelung wird *Disk Duplexing* genannt (Abbildung 8.18). Disk Duplexing ist zudem schneller als Drive Mirroring, da nicht mehr ein Controller die Daten doppelt schreiben muss.

Auch wenn Duplexing schneller als Mirroring ist, sind beide doch langsamer als die klassische Lösung mit einer Festplatte an einem Controller. Sie können auch mehrere Laufwerke verwenden, um Ihre Festplattenzugriffsgeschwindigkeit zu erhöhen. Bei *Disk Striping* (ohne Parität) werden die Daten über mehrere (mindestens zwei) Laufwerke verteilt. Disk Striping allein sorgt also für keinerlei Redundanz. Wenn Sie z.B. eine kleine Textdatei speichern, dann findet eine Aufteilung der Datei in mehrere Teile

statt, wobei die eine Hälfte auf dem einen und die andere auf dem anderen Laufwerk gespeichert wird (Abbildung 8.19).

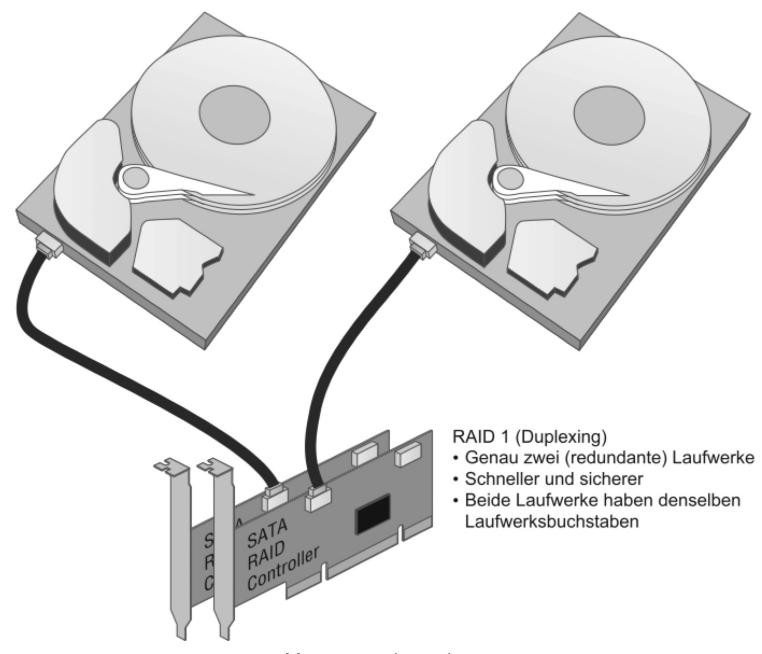


Abb. 8.18: Disk Duplexing

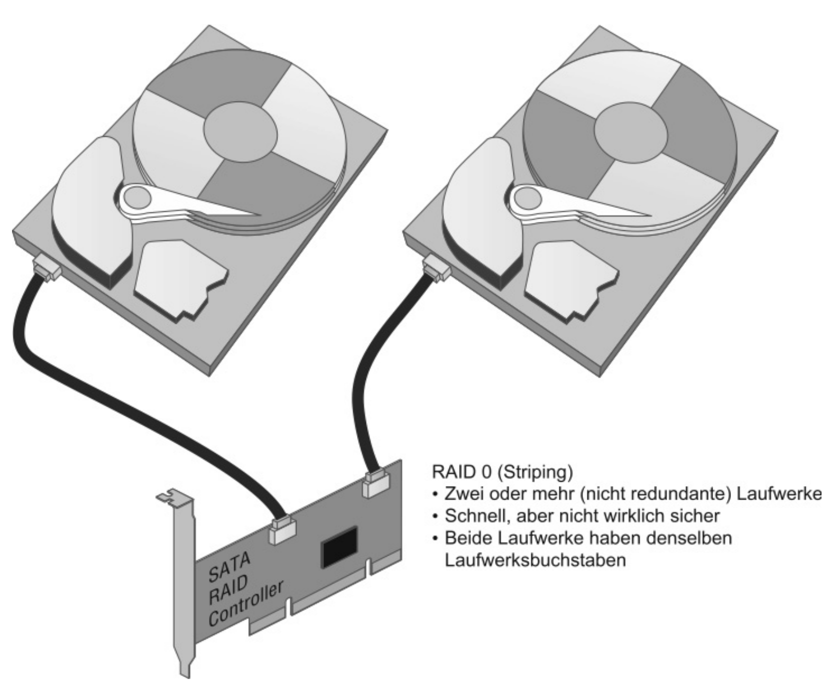


Abb. 8.19: Disk Striping

Der einzige Vorteil von Disk Striping ist dessen Geschwindigkeit, da Daten schneller gelesen und geschrieben werden können, wenn dafür abwechselnd mehrere Laufwerke benutzt werden. Wenn aber auch nur eines der Laufwerke ausfällt, dann gehen damit *alle* Daten verloren. Disk Striping bringt aus dieser Sicht keine Vorteile – es sei denn, Sie sind bereit, für die gesteigerte Geschwindigkeit eine höhere Gefahr des Datenverlustes in Kauf zu nehmen.

Hinweis

Er ist zwar durch Benchmarkprogramme messbar, aber in der Praxis werden Sie keinen Geschwindigkeitsunterschied zwischen Spiegelung und Striping bemerken.

Disk Striping mit Parität schützt im Unterschied dazu die Daten. Dabei werden zusätzliche Informationen erzeugt (*Paritätsdaten*), die beim Ausfall eines Laufwerks dazu benutzt werden können, um die Daten zu rekonstruieren. Für Disk Striping mit Parität werden mindestens drei Laufwerke benötigt, oft werden aber auch mehr verwendet. Disk Striping mit Parität kombiniert die Vorteile von Disk Mirroring und einfachem Disk Striping. Es schützt die Daten und ist ziemlich schnell. Die Mehrzahl der Netzwerkserver arbeitet mit einer Variante von Disk Striping mit Parität.

Hinweis

Es gibt auch eine Bezeichnung für ein Speichersystem, das einfach nur aus einer Reihe unabhängiger Laufwerke verschiedener Größe besteht, nämlich *JBOD*. Die Abkürzung steht für *Just A Bunch Of Disks* (*Einfach nur ein Haufen Festplatten*). Viele Laufwerk-Controller unterstützen auch JBOD.

8.3.1 RAID

Ein paar kluge Köpfe in Berkeley haben in den 1980er-Jahren zahlreiche Techniken für den Einsatz mehrerer Laufwerke entwickelt, um Daten zu schützen und die Geschwindigkeiten zu erhöhen – auch als *RAID* (*Redundant Array of Independent (oder auch Inexpensive) Disks*) bezeichnet. Bei einem Array handelt es sich im RAID-Kontext um einen aus zwei oder mehr Festplatten bestehenden Verbund. Die Entwickler entwarfen sieben RAID-Level, die von 0 bis 6 durchnummeriert wurden (und außerdem einige spezielle Implementierungen). Heutzutage sind nur einige wenige dieser RAID-Typen in Gebrauch: 0, 1, 5, 6, 10 und 0+1.

- **RAID 0 (Disk Striping)**: Hier werden mindestens zwei Laufwerke benötigt. Daten werden *nicht* redundant gespeichert. Wenn eines der Laufwerke ausfällt, gehen *alle* Daten verloren.
- **RAID 1 (Disk Mirroring/Duplexing; Gespiegelte Datenträger)**: Hier werden mindestens zwei Festplatten benötigt, das Spiegeln funktioniert aber auch mit einer beliebigen geraden Anzahl von Festplatten. RAID 1 bietet die beste Datensicherheit, kostet aber eine Menge Speicherplatz, da die Daten doppelt gespeichert (dupliziert) werden. Es werden also zwei 2-TB-Laufwerke benötigt, um 2 TB Daten speichern zu können.
- **RAID 5 (Disk Striping mit verteilter Parität)**: Anstelle Laufwerke eigens für Daten oder Paritätsdaten abzustellen, werden diese bei RAID 5 gleichmäßig über alle Laufwerke verteilt. Das ist das schnellste Verfahren zur Erzeugung von Datenredundanz. Bei RAID 5 handelt es sich um die bei Weitem verbreitetste RAID-Implementation. Es werden mindestens drei Laufwerke benötigt. Die Menge der redundanten RAID-5-Daten bleibt auf die Kapazität eines Laufwerks beschränkt. Wenn Sie z.B. drei 2-TB-Laufwerke verwenden, dann beträgt deren Gesamtspeicherkapazität 4 TB. Wenn Sie vier 2-TB-Laufwerke einsetzen, dann beträgt die Gesamtspeicherkapazität 6 TB.

Hinweis

RAID 5 hört sich theoretisch toll an und macht sich gut in der CompTIA A+Prüfung, ist aber heutzutage in Ungnade gefallen. Die Ausfallrate von Festplatten und deren große Kapazität (die lange Wiederherstel-

lungszeiten verursacht) hat dazu geführt, dass bei den meisten RAID-Implementierungen auf RAID 5 verzichtet wird.

- **RAID 6** (**Disk Striping mit zusätzlicher Parität**): Wenn in einem RAID-5-Array eine Festplatte ausfällt, sind Ihre Daten sehr gefährdet, bis Sie die fehlerhafte Festplatte ersetzen und das Array neu aufbauen. RAID 6 entspricht RAID 5, allerdings mit zusätzlicher Paritätsinformation. RAID 6 benötigt mindestens vier Laufwerke, aber es entstehen keine Probleme, wenn zwei Laufwerke gleichzeitig ausfallen.
- **RAID 10** (**Striping gespiegelter Laufwerke**): Man hat verschiedene RAID-Level miteinander kombiniert, um in den gleichzeitigen Genuss verschiedener Vorteile zu gelangen (Geschwindigkeit, Speicherkapazität, Zuverlässigkeit), muss aber einen Preis dafür zahlen, und das ist die Effizienz. Betrachten Sie beispielsweise RAID 10, das auch als RAID 1+0 oder als »Striping gespiegelter Datenträger« bezeichnet wird. Dafür sind mindestens vier Laufwerke erforderlich. Jeweils zwei werden als gespiegeltes Laufwerk konfiguriert und es ergeben sich zwei RAID-1-Verbunde. Diese erscheinen dem Betriebssystem oder dem Laufwerk-Controller jeweils wie ein einzelnes Laufwerk. Mit diesen beiden »einzelnen« Laufwerken wird dann ein Disk Striping (RAID 0) eingerichtet. Cool, oder? Man erzielt die Geschwindigkeit des Disk Stripings und die Zuverlässigkeit einer Spiegelung, muss dafür jedoch den Preis zahlen, dass für jedes gespeicherte Byte zwei Byte an Speicherkapazität erforderlich sind. Und wenn mehr Speicherplatz benötigt wird, fügen Sie dem Striping-Array einfach ein weiteres Paar gespiegelter Laufwerke hinzu!
- **RAID 0+1** (**Spiegelung gestripter Laufwerke**): Wie bei RAID 10 werden auch bei RAID 0+1 mehrere Verbunde von Festplatten eingesetzt, allerdings in umgekehrter Richtung. Hier sind mindestens vier Laufwerke erforderlich. Zunächst richten Sie zwei RAID-0-Arrays ein, die dann zu einer Festplattenspiegelung verknüpft werden. Welche Methode halten Sie für besser: RAID 10 oder RAID 0+1? Recherchieren Sie doch ein wenig im Internet und entscheiden Sie selbst!

Wichtig

Als Teil der Prüfungsvorbereitung sollten Sie sich mit den RAID-Leveln 0, 1, 5 und 10 vertraut machen, die Anzahl benötigter Laufwerke kennen und wie viele Ausfälle ein Verbund verkraften kann und dennoch weiterhin funktioniert. Diese Informationen sind in der nachstehenden Tabelle zusammengefasst.

RAID-Level	Anzahl benötigter Laufwerke	Erlaubte Anzahl von Laufwerksausfällen
RAID 0	2	0
RAID 1	2	1
RAID 5	3	1
RAID 6	4	2
RAID 10	4	Bis zu 2

8.3.2 RAID implementieren

Die RAID-Level beschreiben verschiedene Verfahren, die für Datenredundanz sorgen und/oder den Datendurchsatz beim Ansprechen der Festplatten erhöhen. Die RAID-Level legen aber nicht fest, *wie* diese Verfahren implementiert werden. Es gibt buchstäblich Tausende verschiedene Methoden zur Einrichtung von RAID. Welche Verfahren verwendet werden, hängt weitgehend vom einzusetzenden RAID-Level, dem verwendeten Betriebssystem und vom Umfang des Budgets ab.

Der sinnvolle Einsatz von RAID beginnt offensichtlich damit, dass mindestens zwei Festplatten irgendwie zu einem RAID-Array gekoppelt werden. Spezielle RAID-Controller unterstützen RAID-

Verbunde von bis zu 15 Laufwerken. Das reicht aus, um auch anspruchsvolleren Anwendungen Rechnung zu tragen. Es gibt fertige Geräte mit RAID-Speicherlösungen, die eine einfache Lösung für externen Speicher oder Backups darstellen.

Wenn Sie also mit mehreren Laufwerken einen RAID-Verbund einrichten möchten, stellt sich die Frage, ob man zur Steuerung Hardware oder Software einsetzt. Sehen wir uns die beiden Möglichkeiten an!

8.3.3 Hardware- vs. Software-RAID

Alle RAID-Implementationen stützen sich entweder auf Hardware- oder Softwareverfahren. Software wird häufig dann eingesetzt, wenn der Preis wichtiger als die Leistung ist. Hardware wird dann eingesetzt, wenn Geschwindigkeit und Datenredundanz gefragt sind. Für Software-RAID werden keine speziellen Controller benötigt. Sie können normale SATA-Controller einsetzen, um ein Software-RAID-Array zu implementieren. Aber Sie benötigen »clevere« Software. Die bekannteste Software-Implementation von RAID ist die in Windows integrierte RAID-Software. Mit der Datenträgerverwaltung in Windows-Serverversionen können Sie Laufwerke für RAID 0, 1 oder 5 konfigurieren und sie unterstützt PATA oder SATA (Abbildung 8.20). Die Datenträgerverwaltung in Windows 7/8/8.1/10 unterstützt RAID 0 und 1.

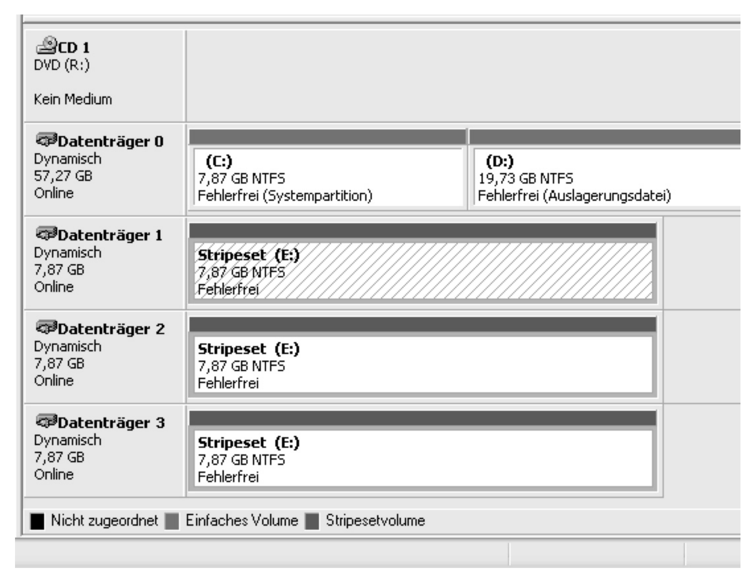


Abb. 8.20: Datenträgerverwaltung in Windows

Hinweis

In Kapitel 9, *Vorbereitung und Wartung von Festplatten*, werden die in Windows implementierten RAID-Lösungen erörtert.

Nicht nur die Windows-Datenträgerverwaltung unterstützt Software-RAID. Es gibt eine Reihe Softwarelösungen von Drittanbietern, die auch unter anderen Betriebssystemen eingesetzt werden können.

Software-RAID bedeutet, dass das Betriebssystem für alle RAID-Funktionen zuständig ist. Es eignet sich zwar für kleine RAID-Lösungen, führt aber zu gewissen Belastungen des Betriebssystems und beeinträchtigt die Systemleistung. Wenn Sie RAID *ernsthaft* nutzen wollen, damit nicht einmal die Benutzer bemerken, dass Probleme aufgetreten sind, dann bietet nur Hardware-RAID die entsprechende Lösung.

Hinweis

In Kapitel 9 werde ich ausführlich auf die in Windows 8/8.1/10 verfügbare RAID-Implementierung *Speicherplätze* eingehen.

Hardware-RAID ist auf einen intelligenten Controller angewiesen, der für alle RAID-Funktionen zuständig ist (Abbildung 8.21). Im Unterschied zu normalen PATA/SATA-Controllern besitzen diese Controller eigene Prozessoren und eigenen Speicher, um anstelle des Betriebssystems alle Aufgaben im Zusammenhang mit der RAID-Implementierung bewältigen zu können.

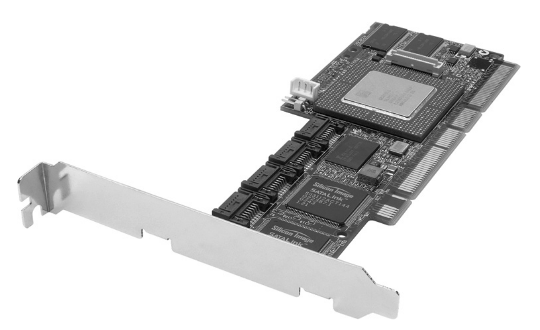


Abb. 8.21: Ein SATA-RAID-Controller

Bei den meisten in der Praxis eingesetzten RAIDs handelt es sich um Hardwarelösungen. Es gibt eine ganze Reihe verschiedener RAID-Hardwarelösungen, die fast ausnahmslos *Hot-Swapping* unterstützen, damit einzelne defekte Laufwerke auch während des laufenden Betriebs des Rechners ausgetauscht werden können. Hot-Swapping wird von RAID-Hardwarelösungen daher üblicherweise unterstützt.

Eine RAID-Hardwarelösung ist für das Betriebssystem unsichtbar und wird in Abhängigkeit von den jeweils beteiligten Chips unterschiedlich konfiguriert. Bei den meisten RAID-Systemen enthält das Flash-ROM ein spezielles Konfigurationsprogramm, das Sie nach dem Abarbeiten der CMOS-Programme, aber vor dem Laden des Betriebssystems aufrufen können. Abbildung 8.22 zeigt ein typisches Firmware-Programm, das zur Konfiguration einer RAID-Hardwarelösung verwendet wird.

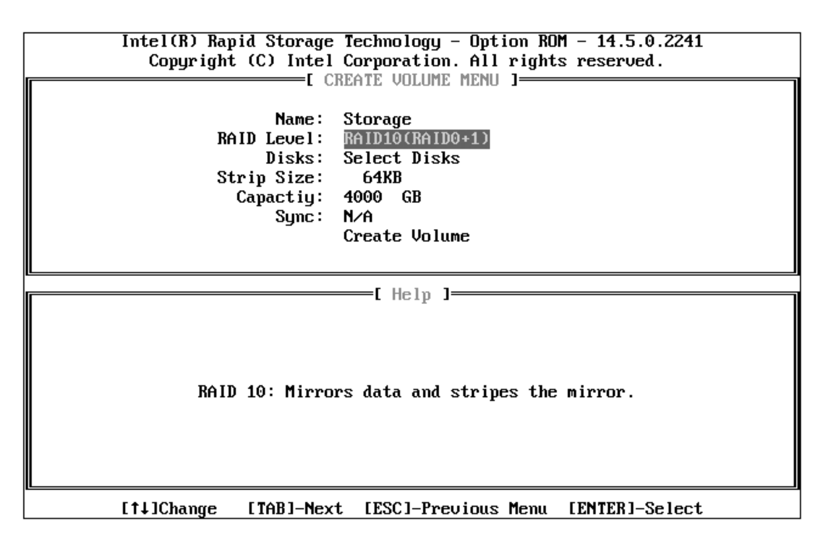


Abb. 8.22: RAID-Konfigurationsprogramm

Tipp

Probieren Sie unter `http://totalsem.com/100x` die Übung zu Kapitel 8 aus, um den besten Kompromiss zwischen Speicherkapazität und Geschwindigkeit eines RAID-Verbunds zu ermitteln.

8.3.4 RAID-Komplettsysteme

Viele Anwender benutzen RAID-Komplettsysteme, die ihnen zusätzlichen Speicherplatz und einen Ort für Dateibackups bieten. In diesen Geräten sind zwei oder mehr Laufwerke eingebaut. Sie werden mit einem der Anschlüsse des Computers verbunden, wie USB oder Thunderbolt (bei neueren Systemen) oder FireWire oder eSATA (bei älteren Systemen). Details zu USB und FireWire finden Sie in Kapitel 10. Abbildung 8.23 zeigt ein externes RAID-Komplettsystem. Dieses typische Modell bietet für die beiden darin installierten Laufwerke drei Optionen: kein RAID, RAID 0 oder RAID 1.



Abb. 8.23: RAID-System von Western Digital

8.4 Laufwerke installieren

Die Installation eines Laufwerks ist relativ einfach, wenn Sie sich die Zeit nehmen, um das richtige Laufwerk für Ihr System auszuwählen, das Laufwerk korrekt zu konfigurieren und einige schnelle Tests durchzuführen, die zeigen, ob es einwandfrei läuft. Weil es für PATA und SATA unterschiedliche Verkabelungsanforderungen gibt, werden wir sie einzeln betrachten.

Wichtig

Lassen Sie sich bei den Prüfungsvorbereitungen nicht vom Textumfang der Erklärung der Installation abschrecken. Die PATA-Installation ist sehr viel komplizierter als die SATA-Installation, deshalb ist ihr mehr Raum gewidmet. In der Praxis und in der Prüfung wird Ihnen höchstwahrscheinlich eher SATA begegnen.

8.4.1 Auswahl des Laufwerks

Als Erstes müssen Sie entscheiden, wo Sie das Laufwerk anschließen wollen. Wenn Sie ein neues Mainboard verwenden, können Sie ein M.2-Laufwerk direkt in den passenden Anschluss einsetzen

und mit einer kleinen Schraube sichern. Wenn Sie eine 3,5-Zoll-HDD oder eine 2,5-Zoll-SSD installieren möchten, ist es etwas umständlicher. Suchen Sie nach einem freien SATA-Anschluss. Gehört er zu einem eigenen RAID-Controller? Viele Mainboards mit eingebauten RAID-Controllern haben eine CMOS-Einstellung, über die Sie RAID aktivieren und deaktivieren können (Abbildung 8.24).

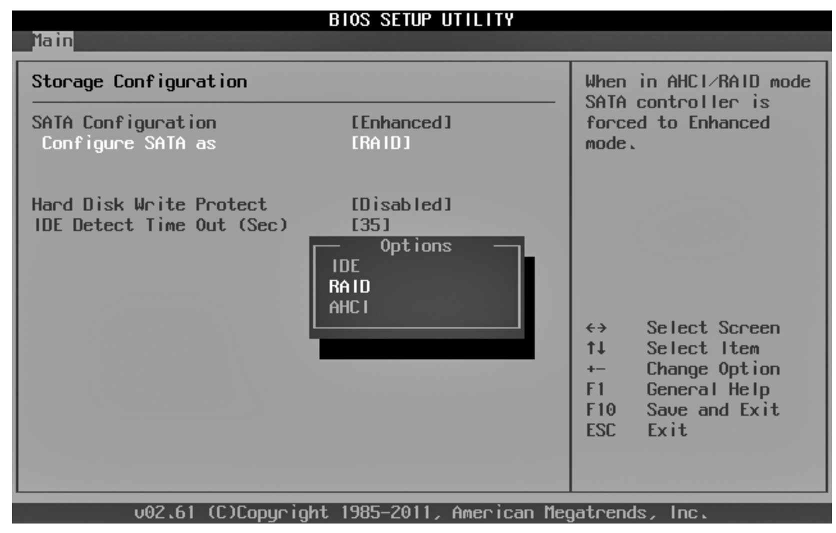


Abb. 8.24: RAID-Einstellungen im CMOS-Setup

Zweitens müssen Sie prüfen, ob genügend Platz für das Laufwerk im Gehäuse ist. Wo wollen Sie es einbauen? Haben Sie einen freien Stromanschluss? Reichen die Daten- und Stromkabel bis zum Laufwerk? Es ist immer sinnvoll, zuerst zu testen, ob alles passt.

Tipp: Wärmeentwicklung durch mehrere Laufwerke

Der Einbau von drei oder mehr Laufwerken in ein enges PC-Gehäuse kann gefährlich werden, wenn man nicht aufpasst! Die erzeugte Wärme verändert zwar nicht die Struktur des Raumzeitkontinuums, es ist aber erwiesen, dass die Wärme die Lebensdauer von Laufwerken und Computern verringert. Bei einem mit einem RAID-Verbund ausgestatteten System müssen Sie sich der Wärmeentwicklung annehmen, weil die Anzahl der Laufwerke in solchen Systemen für gewöhnlich erheblich größer ist als in den meisten anderen Computern. Am einfachsten ist es, zu diesem Zweck Lüfter einzubauen.

Öffnen Sie das Gehäuse und suchen Sie nach für die Aufnahme von Lüftern vorbereiteten Stellen. Wie viele Lüfter sind bereits installiert? Von welcher Größe sind sie? Welche Größe können Sie verwenden? (In den meisten Gehäusen kommen Lüfter mit einem Durchmesser von 80 mm zum Einsatz, 120 mm oder noch größer sind jedoch ebenfalls gebräuchlich.) Notieren Sie sich die Eigenheiten Ihres Systems und besuchen Sie den örtlichen Computerhändler oder einen Onlineshop, um passende Lüfter zu besorgen.

Bevor Sie aber ohne groß nachzudenken nach dem erstbesten großen Lüfter greifen, sollten Sie sich über die zusätzliche Geräuschentwicklung Gedanken machen. Versuchen Sie, einen Kompromiss zwischen kühlem Rechnergehäuse und verfrühter Taubheit zu finden.

8.4.2 Installation von PATA-Laufwerken

Es tut mit leid, aber die CompTIA verlangt noch immer Kenntnisse über PATA-Laufwerke (IDE), deshalb wollen wir die Installation dieser uralten Geräte schnell abhandeln. Wenn Sie nur ein Festplattenlaufwerk verwenden, setzen Sie die Jumper des Laufwerks auf Master oder Standalone. Falls Sie zwei

Laufwerke benutzen, setzen Sie eines auf Master, das andere auf Slave oder beide auf Cable Select. Abbildung 8.25 zeigt eine Nahaufnahme eines PATA-Festplattenlaufwerks mit den Jumpern.

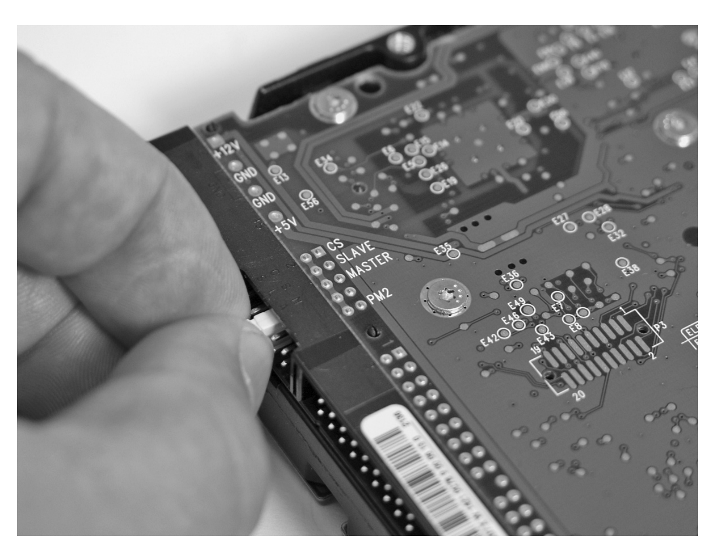


Abb. 8.25: Master/Slave-Jumper einer PATA-Festplatte

Zunächst einmal müssen Sie vielleicht feststellen, dass die Jumper nicht mit *Master* und *Slave* beschriftet sind. Woher wissen Sie also, dass Sie diese richtig gesetzt haben? Am einfachsten ist es, auf dem Laufwerk selbst nachzusehen. Bei den meisten Laufwerken gibt es ein Diagramm, das erläutert, wie die Jumper korrekt gesetzt werden müssen. Abbildung 8.26 zeigt einen solchen Aufkleber, der Ihnen mitteilt, wie das Laufwerk als Master, als Slave oder für Cable Select eingerichtet werden muss.

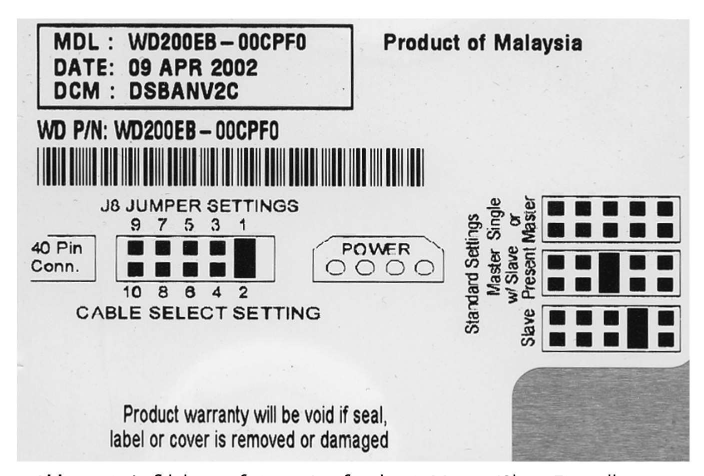


Abb. 8.26: Aufkleber auf einem Laufwerk mit Master/Slave-Einstellungen

Festplattenkabel haben einen farbigen Streifen, der dem *Pin 1* am Stecker entspricht. Sie müssen dafür sorgen, dass Pin 1 am Controller und Pin 1 am Laufwerk dieselbe Ader verwenden. Wenn Sie das Laufwerk nicht korrekt anschließen, kann der PC das Laufwerk auch nicht erkennen. Wenn Sie die Master/Slave-Jumper nicht richtig setzen oder das Laufwerk falsch verkabeln, geht nichts kaputt – es funktioniert nur nicht.

Auf älteren Mainboards gibt es eigene PATA-Anschlüsse, an die Sie das PATA-Kabel direkt anschließen können. Auf neueren Mainboards gibt es diese Anschlüsse nicht, deshalb benötigen Sie eine Erweiterungskarte mit einem PATA-Controller, um ein PATA-Laufwerk anzuschließen.

Und schließlich müssen Sie einen Molex-Stecker vom Netzteil mit dem Laufwerk verbinden. Alle PATA-Laufwerke verwenden Molex-Stecker. So viel zum Anschluss von PATA-Laufwerken.

8.4.3 Verkabelung von SATA-Laufwerken

Die Installation von SATA-Festplattenlaufwerken ist viel einfacher als die Installation von PATA-Laufwerken, weil es keine Jumper-Einstellungen gibt, bei denen Sie etwas falsch machen könnten, weil SATA nur ein einziges Laufwerk pro Controller-Kanal unterstützt. Sie schließen einfach die Stromversorgung an und verbinden das Datenkabel wie in Abbildung 8.27. Dann erkennt das Betriebssystem das Laufwerk automatisch, und Sie können es sofort benutzen! Die Form der Anschlüsse für die Datenleitung und die Stromversorgung verhindert, dass Sie etwas falsch anschließen.

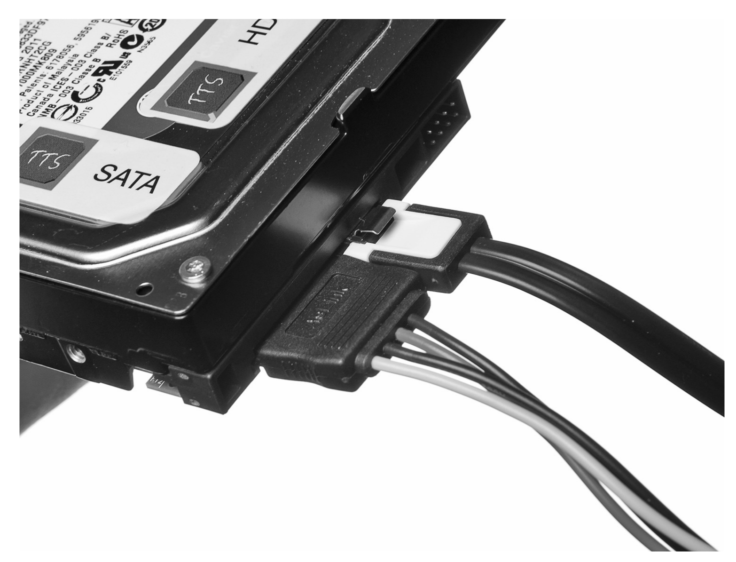


Abb. 8.27: Korrekt angeschlossene Kabel an einem SATA-Laufwerk

Hinweis

Bei einigen älteren SATA-Laufwerken gibt es Jumper, die aber zur Konfiguration der SATA-Version (1.5, 3.0) oder der Stromversorgung verwendet werden. Die Regel »pro Controller ein Laufwerk« gilt für diese Laufwerke ebenso wie für die häufigeren SATA-Laufwerke ohne Jumper.

Alle modernen Mainboards verfügen über zwei oder mehr SATA-Anschlüsse, wie Sie aus Kapitel 6, *Mainboards*, wissen. Typischerweise wird das primäre Laufwerk als SATA 1, das nächste als SATA 2 usw. installiert. Bei SATA-Laufwerken, von denen nicht gebootet wird, wie bei Mainboards mit M.2-Anschlüssen, spielt es keine Rolle, mit welchem Anschluss das Laufwerk verbunden wird.

8.4.4 Anschluss von SSDs

SATA-SSDs verfügen über die gleichen Anschlüsse wie magnetische SATA-Laufwerke. Die meisten SATA-SSDs besitzen ein 2,5-Zoll-Gehäuse. Wie bei den älteren Festplattenvarianten funktionieren sie korrekt, wenn sie richtig angeschlossen sind, oder eben gar nicht, wenn sie falsch angeschlossen wurden.

M.2- und mSATA-Laufwerke werden am entsprechenden Steckplatz auf dem Mainboard oder einer zusätzlichen Steckkarte angeschlossen. Sie rasten dort ein oder werden mit einer winzigen Schraube befestigt (Abbildung 8.28). Beide Standards verwenden einen eigenen Anschluss, daher besteht keine Gefahr, sie falsch zu installieren.

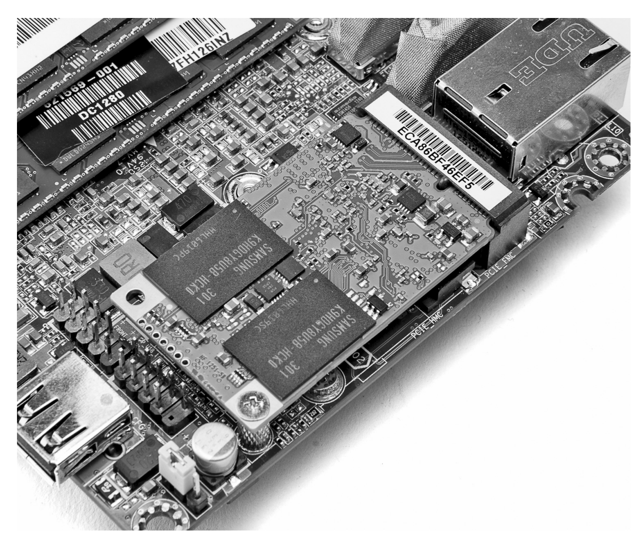


Abb. 8.28: Auf dem Mainboard befestigte mSATA-SSD

Denken Sie vor dem Installieren oder Ersetzen einer vorhandenen HDD durch eine SSD an die folgenden Dinge:

- Haben Sie die passenden Treiber und geeignete Firmware für die SSD? Neuere Windows-Versionen laden die aktuellen Treiber automatisch herunter. Wie üblich, sollten Sie auch hier genau auf die Herstellerangaben achten.
- Sie haben alle wichtigen Daten gesichert? Gut!

8.5 BIOS-Unterstützung: CMOS-Einstellungen und Treiberinstallation

Alle Komponenten in Ihrem PC sind auf BIOS-Unterstützung angewiesen, sei es nun das herkömmliche BIOS oder UEFI. Laufwerk-Controller bilden hier keine Ausnahme. Mainboards unterstützen die SATA-Laufwerk-Controller über das System-BIOS, aber häufig müssen Sie für die jeweils installierten Festplatten CMOS-Einstellungen vornehmen.

In der guten alten Zeit musste man das CMOS-Setup aufrufen und bei der Installation manuell Informationen über das neue Laufwerk eingeben. Dieser Vorgang findet heutzutage automatisiert statt.

8.5.1 Controller konfigurieren

Bei der Konfiguration von Controllern sollten Sie sich als Erstes davon überzeugen, dass sie aktiviert sind. Die meisten Controller bleiben aktiviert und sind stets bereit, automatisch neue Laufwerke zu erkennen, sie lassen sich jedoch im CMOS auch leicht deaktivieren. Gehen Sie Ihre CMOS-Einstellungen durch, um die Optionen für das Aktivieren/Deaktivieren der Controller zu finden (eine typische Einstellung finden Sie in Abbildung 8.29). Hier sollten Sie auch prüfen, ob Ihre Onboard-RAID-Controller sowohl mit RAID- als auch mit anderen Einstellungen funktionieren.

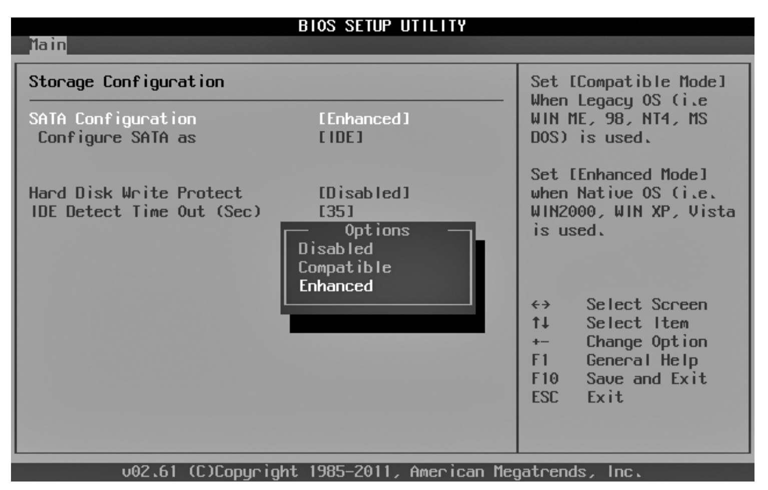


Abb. 8.29: Typische Controller-Einstellungen im CMOS-Setup

8.5.2 Automatische Erkennung (Autodetection)

Wenn die Controller aktiviert sind und das Laufwerk korrekt angeschlossen ist, sollte das Laufwerk automatisch erkannt werden und im CMOS-Setup angezeigt werden (*Autodetection*). Die automatische Erkennung ist eine leistungsfähige und praktische Funktion, die Ihnen nahezu die gesamte Arbeit bei der Konfiguration einer Festplatte abnimmt.

Mainboards verwenden ein Nummerierungssystem, um festzulegen, wie Laufwerke aufgelistet werden – aber jedes Mainboard nutzt ein anderes System! Bei einem üblichen Verfahren werden die einzelnen Controller *Channel* (*Kanäle*) genannt. Standardmäßig wird erst versucht, über Channel 1 zu booten, dann über Channel 2 usw. Statt Laufwerksbezeichnungen werden jetzt also Zahlen angezeigt. Betrachten Sie dazu auch Abbildung 8.30.

Puh! Jede Menge Festplattenlaufwerke! Dieses Mainboard unterstützt sechs SATA-Laufwerke. Jedem Controller ist eine Nummer zugewiesen, eine M.2-SSD an SATA 0, Festplattenlaufwerke an SATA 1 und SATA 2 sowie das optische Laufwerk an SATA 3. Alle Laufwerke wurden vom BIOS automatisch erkannt und eingerichtet, ohne dass ich irgendetwas einstellen musste. Schöne neue Welt!

8.5.3 Bootreihenfolge

Wenn Sie Ihren Computer starten wollen, braucht er ein Betriebssystem, das er booten kann. In welcher Reihenfolge er versucht, von den vorhandenen Laufwerken zu starten, wird im CMOS-Setup festgelegt.

Abbildung 8.31 zeigt einen typischen Bildschirm für die Festlegung der Bootreihenfolge. Es gibt hier eine erste, eine zweite und eine dritte Option. Viele Benutzer wollen zuerst von einem optischen Laufwerk und dann von einer Festplatte booten. Auf diese Weise können sie bei Systemproblemen zum Starten des Rechners eine bootfähige optische Disc einlegen. Natürlich können Sie auch festlegen, dass als Erstes von der Festplatte gebootet wird, und die Einstellungen im CMOS-Setup bei Bedarf entsprechend ändern. Aber das bleibt ganz Ihnen überlassen.

Bei den meisten modernen CMOS-Setup-Programmen gibt es einen weiteren Bildschirm, auf dem eine Bootreihenfolge nur für Festplatten festgelegt wird. Wenn Sie beispielsweise als Bootreihenfolge erst optisches Laufwerk, dann Festplatte und zuletzt USB-Stick konfiguriert haben, von welchem Laufwerk soll das System dann starten, wenn Sie über mehr als eine Festplatte verfügen? Auf diesem Bildschirm können Sie das einstellen. Falls sich auf jeder Festplatte ein anderes Betriebssystem befindet, ist das äußerst praktisch.

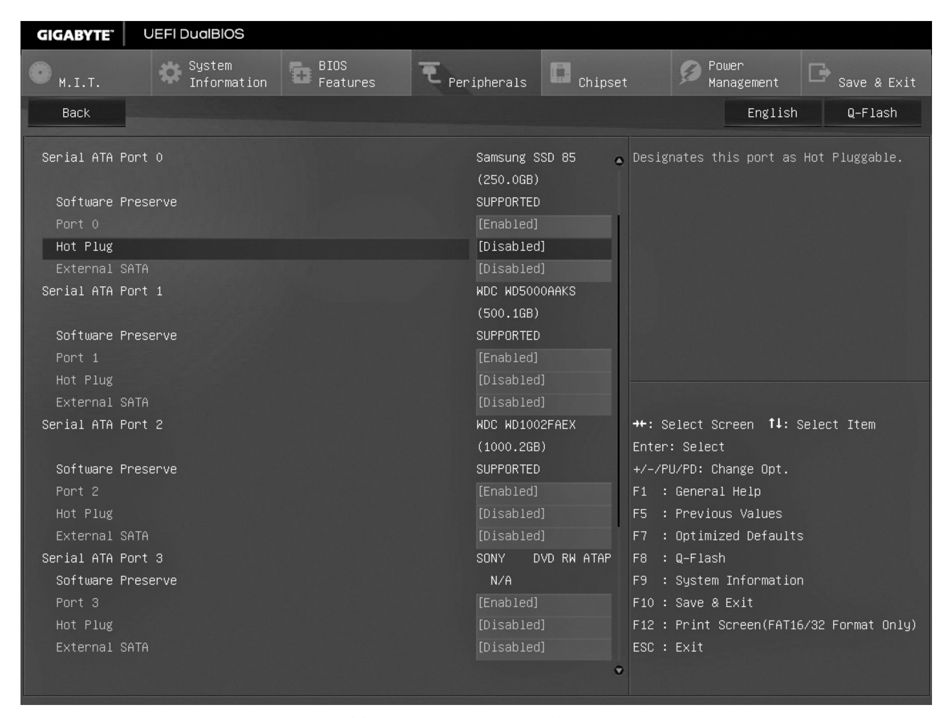


Abb. 8.30: CMOS-Einstellungen

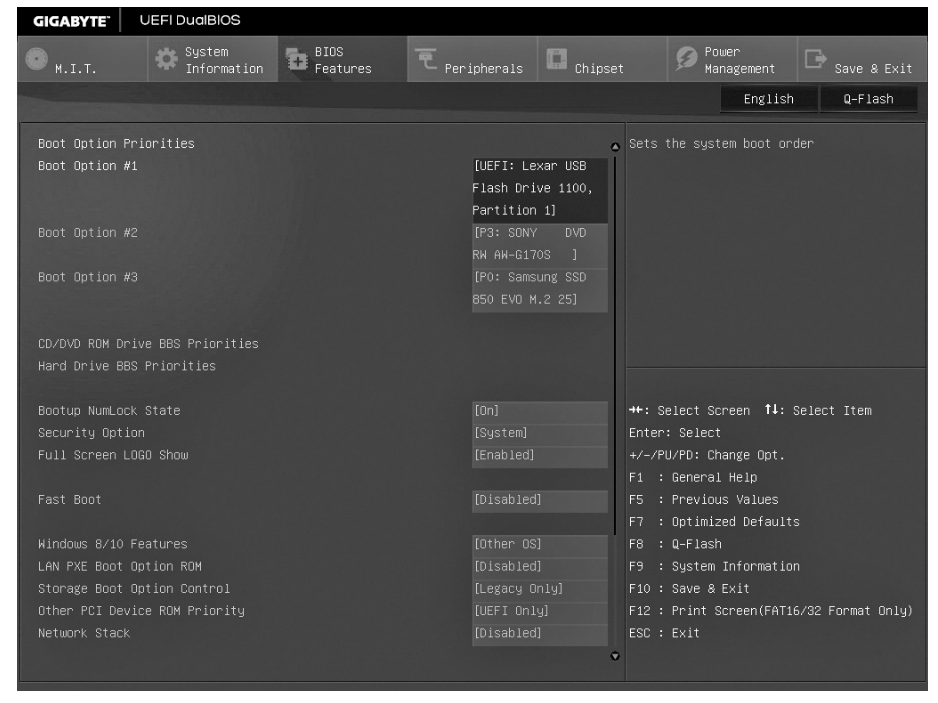


Abb. 8.31: Bootreihenfolge

8.5.4 AHCI aktivieren

Bei Mainboards mit AHCI-Unterstützung aktivieren Sie diese über das CMOS-Setup. Im Allgemeinen stehen Ihnen bis zu drei Optionen zur Auswahl: IDE/SATA OR COMPATIBILITY MODE, AHCI oder RAID. Den Kompatibilitätsmodus verwenden Sie bei der Installation älterer Betriebssysteme wie Windows XP. Für HDDs und SSDs ist AHCI am besten geeignet, aktivieren Sie also die AHCI-Option für den HBA.

8.6 Fehlersuche bei der Festplatteninstallation

Der beste Freund des Technikers bei der Problembehebung einer Festplatteninstallation ist die automatische Erkennung im CMOS-Setup. Wenn ein Laufwerk nicht funktioniert, dann lautet die größte Frage, speziell bei der Installation: »Habe ich es korrekt angeschlossen?« oder »Habe ich Strom- und Datenkabel richtig angeschlossen?« Bei automatischer Erkennung fällt die Antwort leicht, denn wenn dabei eines der Laufwerke nicht erkannt wird, dann stimmt mit der Hardwarekonfiguration etwas nicht. Entweder ist das Laufwerk physisch defekt oder, was wahrscheinlicher ist, Sie haben vergessen, das Stromkabel anzuschließen, das Datenkabel nicht richtig eingesteckt oder beim Herstellen der Verbindung irgendetwas anderes durcheinandergebracht. Gehen Sie bei der Fehlersuche der Reihe nach alle Installationsschritte durch, um herauszufinden, was schiefgegangen ist.

Vergewissern Sie sich, dass das BIOS Ihr Laufwerk erkennt. Verwenden Sie das CMOS-Setup-Programm, um das festzustellen. Überprüfen Sie die physischen Verbindungen und sehen Sie im CMOS-Setup-Programm nach, ob der Controller aktiviert ist. Oder unterstützt das Mainboard überhaupt den Laufwerkstyp, den Sie zu installieren versuchen? Falls das nicht der Fall ist, stehen Ihnen verschiedene Optionen zur Verfügung. Möglicherweise können Sie vom Hersteller des Mainboards eine neuere BIOS-Version erhalten und es aktualisieren. Oder Sie beschaffen sich einen Laufwerk-Controller in Form einer Steckkarte, der Ihr Gerät unterstützt.

8.7 Wiederholung

8.7.1 Fragen

1. Welche der nachfolgenden Rotationsgeschwindigkeiten ist für eine HDD gebräuchlich?
   A. 5.200 U/min
   B. 7.200 U/min
   C. 9.200 U/min
   D. HDDs besitzen keine beweglichen Teile.
2. Welcher Formfaktor wird direkt an einen speziellen Steckplatz auf dem Mainboard angeschlossen?
   A. 2,5-Zoll-SSD
   B. 3,5-Zoll-SSD
   C. M.2-SSD
   D. eSATA-SSD
3. Wie viele PATA-Laufwerke können Sie an ein System mit zwei PATA-Festplatten-Controllern anschließen?
   A. Eins
   B. Zwei
   C. Drei
   D. Vier

4. Wie unterscheiden Sie zwei PATA-Laufwerke am selben Kabel?
   A. Beim Flachbandkabel sind sieben Leitungen »verdreht«, über die die Laufwerke identifiziert werden.
   B. Durch Setzen von Jumpern am jeweiligen Laufwerk, die Master und Slave festlegen.
   C. Der PATA-Controller bestimmt die Hierarchie.
   D. Beide Laufwerke gelten als gleichberechtigt.
5. Was passiert, wenn Sie ein einzelnes PATA-Festplattenlaufwerk falsch anschließen?
   A. Sie könnten das Laufwerk beschädigen.
   B. Die Daten werden gelöscht, aber die Festplatte nimmt keinen Schaden.
   C. Das System kann nicht mit der Festplatte kommunizieren.
   D. Das Laufwerk wird im Kompatibilitätsmodus installiert.
6. Wie lang darf ein Kabel für ein internes SATA-Gerät maximal sein?
   A. 2 Meter
   B. 30 Zentimeter
   C. 45 Zentimeter
   D. 1 Meter
7. Wie viele SATA-Laufwerke können Sie maximal an ein System anschließen?
   A. Ein Master- und ein Slave-Laufwerk
   B. Zwei, ohne Master/Slave-Unterscheidung
   C. Acht
   D. Es gibt keine Obergrenze außer den Beschränkungen durch Ihr Mainboard.
8. Welche SATA-Version erfordert den geringsten Verwaltungsaufwand (und ist damit am schnellsten)?
   A. AHCI
   B. SATA 2.0
   C. PATA 3.0
   D. SATAe
9. Welcher Standard unterstützt magnetische SATA-Laufwerke am effizientesten?
   A. AHCI
   B. CMOS
   C. SATA-IO
   D. SATA 3.2
10. Welches RAID-Level benötigt mindestens vier Laufwerke?
   A. RAID 1
   B. RAID 4
   C. RAID 5
   D. RAID 10

8.7.2 Antworten

1. **B.** Gängige Rotationsgeschwindigkeiten magnetischer Festplatten sind 5.400, 7.200, 10.000 und 15.000 U/min.
2. **C.** M.2-SSDs (und mSATA-SSDs) werden an einen speziellen Steckplatz angeschlossen.
3. **D.** Jeder Controller unterstützt zwei Laufwerke.

4. **B.** Zur Unterscheidung von zwei PATA-Laufwerken werden Jumper und die Master/Slave-Einstellungen verwendet.
5. **C.** Es wird nichts beschädigt und es geht nichts verloren – das Laufwerk funktioniert einfach nur nicht.
6. **D.** Kabel dürfen bei internen SATA-Geräten maximal einen Meter lang sein.
7. **D.** Es gibt keine Obergrenze für die Anzahl der SATA-Laufwerke, die Sie an ein System anschließen können, außer der durch die Anzahl der Anschlüsse an Ihrem Mainboard/Ihrer Host-Karte vorgegebenen.
8. **D.** SATA Express (SATAe) nutzt den PCIe-Bus, daher entfällt der sonst übliche Verwaltungsaufwand.
9. **A.** Der AHCI-Standard unterstützt magnetische SATA-Laufwerke effizient.
10. **D.** RAID 10 benötigt mindestens vier Laufwerke.

Vorbereitung und Wartung von Festplatten | 9

Themen in diesem Kapitel:

- Partitionstypen
- Formatierungsoptionen
- Partitionierung und Formatierung
- Wartung und Reparatur

Aus der Sicht des Rechners handelt es sich bei einer erfolgreich installierten Festplatte nur um einen riesigen Haufen unorganisierten Speicherplatzes. Das CMOS erkennt das Laufwerk automatisch. So weit es das Betriebssystem betrifft, ist das Laufwerk ohne weitere Informationen aber nicht lesbar. Es muss diesen riesigen unorganiserten Speicherplatz verwalten, damit Sie das Laufwerk zum Speichern von Daten verwenden können. Und genau darum geht es in diesem Kapitel.

Hinweis

Die Begriffe »Festplatte« und »Laufwerk« dienen in diesem Kapitel ganz allgemein zur Beschreibung der verschiedenen in Kapitel 8, *Festplattentechnologien*, erläuterten Gerätetypen. Sobald Windows läuft, ist es dem Betriebssystem ziemlich egal, ob es sich um ein plattenbasiertes Laufwerk (HDD) oder um eine SSD handelt. Die beim Umgang mit diesen Geräten erforderlichen Programme und die verschiedenen Arbeitsschritte bleiben dieselben.

Geschichte und Konzepte

Wenn das Festplattenlaufwerk erfolgreich installiert ist, müssen Sie noch zwei weitere Schritte ausführen, um aus dem Laufwerk und den darin integrierten Schaltungen etwas für den Rechner Brauchbares zu machen: Partitionieren und Formatieren. Beim *Partitionieren* wird das physische Festplattenlaufwerk elektronisch in Gruppen aufgeteilt, die *Partitionen* (oder *Volumes*) genannt werden. Nach der Partitionierung müssen Sie das Laufwerk *formatieren*. Dieser Schritt installiert ein *Dateisystem* auf dem Laufwerk, das die einzelnen Partitionen so organisiert, dass das Betriebssystem darauf Dateien und Ordner speichern kann. Es gibt mehrere verschiedene Dateisysteme, die unter Windows verwendet werden können. Diese werde ich nach der Partitionierung beschreiben.

Die Partitionierung und Formatierung eines Laufwerks ist einer der wenigen verbliebenen Prozesse, die bei der PC-Einrichtung auf der Software-Seite stattfinden und bei dem Sie mehrere relativ komplizierte manuelle Schritte durchführen müssen. Die CompTIA A+-Zertifizierungsprüfungen testen Ihr Wissen, *was* diese Prozesse machen, um ein Laufwerk zum Laufen zu bringen, und ebenso die Schritte, die für die Partitionierung und Formatierung von Festplatten in Windows erforderlich sind.

Dieses Kapitel setzt die Betrachtungen zur Festplatteninstallation fort und erläutert die Partitionierung und die Formatierung. Anschließend wird der Prozess der Partitionierung und Formatierung von Festplatten konkret betrachtet. Das Kapitel endet mit einer Beschreibung der Festplattenwartung und Aspekten der Fehlersuche, die alle in den aktuellen Prüfungen vorkommenden Betriebssysteme umfassen.

9.1 Festplattenpartitionen

Bevor eine magnetische Festplatte die Fabrik verlässt, werden Millionen kleiner magnetischer Speicherbereiche eingerichtet, die als Sektoren bezeichnet werden. (Bei sehr großen Festplatten sind es sogar mehrere Hundert Millionen.) Bei älteren Festplatten waren die Sektoren 512 Byte groß. Moderne Festplatten verwenden 4096-Byte-Sektoren, sogenannte AF-Sektoren (*Advanced Format*). Abbildung 9.1 zeigt einige Sektoren einer typischen HDD.

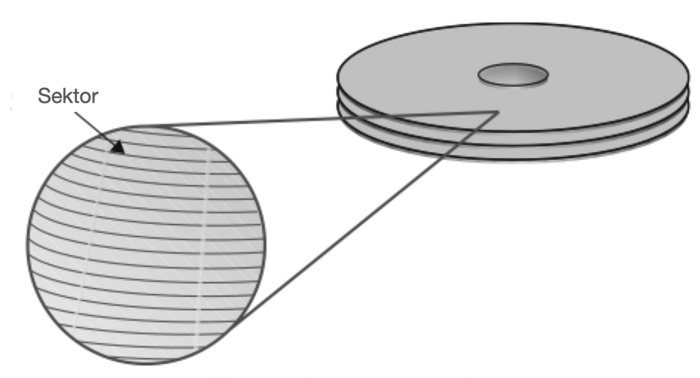


Abb. 9.1: Sektoren einer Festplatte

SSDs enthalten NAND-Chips mit mehreren Millionen 4096 Byte großen Speicherbereichen, die *Seiten* genannt werden. (Bei sehr großen SSDs sind es wieder mehrere Hundert Millionen.) Eine Gruppe von Seiten wird zu einem *Block* zusammengefasst. Die Größe eines Blocks variiert, aber 128 Seiten pro Block sind nicht unüblich. Abbildung 9.2 zeigt ein vereinfachtes Modell des Aufbaus.

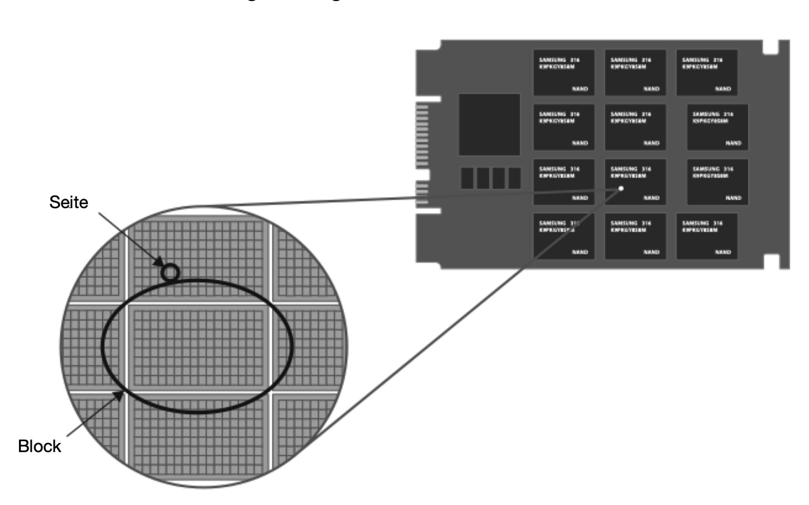


Abb. 9.2: Seiten und Blöcke einer SSD

CPU und Betriebssystem greifen aber nicht direkt auf diese internen Strukturen zu. Vielmehr verwendet der HDD- oder SSD-Controller *LBA* (*Logical Block Addressing*), um den gesamten Speicher in Bereiche aufzuteilen, die mit einer LBA-Adresse durchnummeriert werden, die bei LBA 0 beginnt (Abbildung 9.3). Diese Speicherabschnitte werden ebenfalls als *Blöcke* bezeichnet.

LBA vereinfacht es, alle möglichen Arten von Massenspeicher zu adressieren, deshalb interagiert das Betriebssystem mit Massenspeichern über Blöcke. Dem Benutzer zeigt das Betriebssystem Ordner

und Dateien an, keine LBA-Adressen. Sie müssen den Massenspeicher so organisieren, dass Sie in der Lage sind, Dateien zu erzeugen und abzurufen, Ordner anzulegen usw. Der erste Schritt dabei ist die Partitionierung.

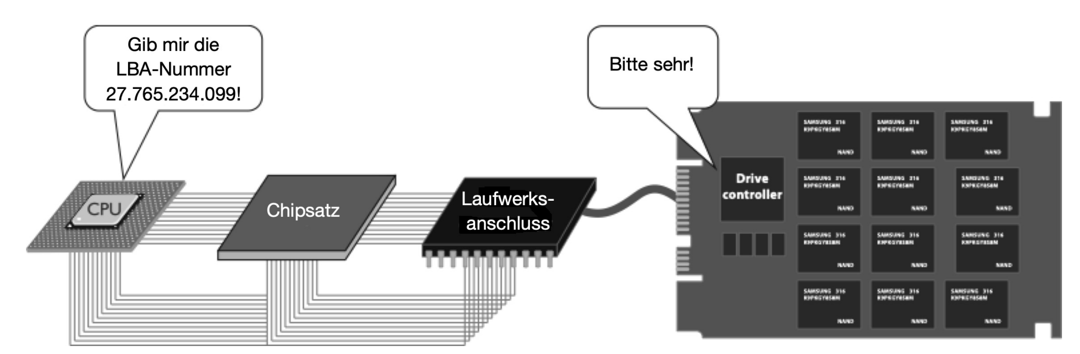


Abb. 9.3: LBA in Aktion

Wenn Sie sich eine Festplatte wie ein großes Gebäude mit vielen Räumen (den Blöcken) vorstellen, dann ist es die Partitionierung, die diese Räume in größere Einheiten (wie z.B. Suiten oder Firmen) unterteilt und diesen Einheiten einen Namen verleiht (Abbildung 9.4). Die Partitionierung organisiert ein einzelnes physisches Laufwerk in Form von mehreren Partitionen. Bei dieser Analogie können Sie sich eine Partition wie eine Zusammenstellung von Räumen im Gebäude vorstellen. Partitionen bieten eine enorme Flexibilität für die Organisation der Festplatten. Mit Partitionen können Sie Laufwerke so einrichten, dass sie genau Ihren persönlichen Anforderungen entsprechen.

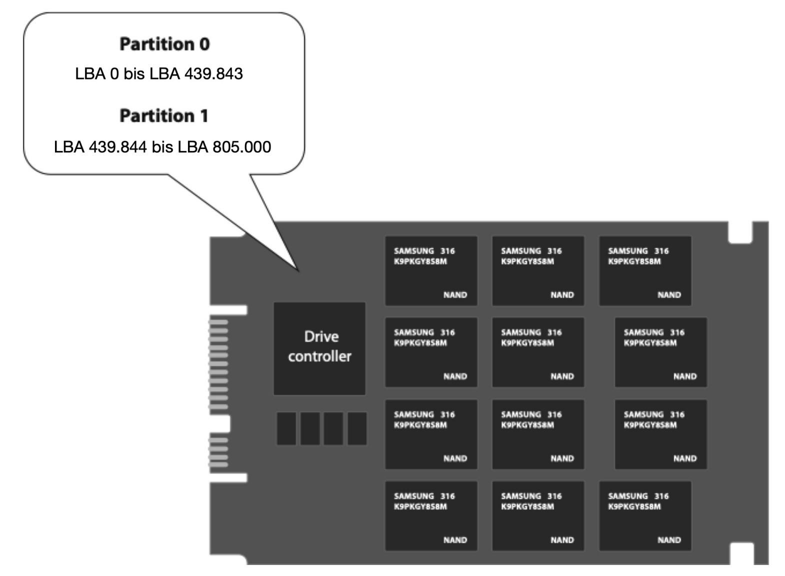


Abb. 9.4: Partitionen eines SSD-Laufwerks

Durch die Partitionierung kann eine einzige Festplatte mehrere Betriebssysteme aufnehmen. Ein Betriebssystem könnte innerhalb von einer Partition untergebracht werden, ein zweites Betriebssystem innerhalb einer anderen Partition. Natürlich benutzen die meisten Leute nur ein Betriebssystem, aber wenn Sie sowohl Windows als auch Linux booten wollen, dann wird dies mit Partitionen möglich.

1002

Windows unterstützt drei unterschiedliche Partitionierungsmethoden: das ältere *MBR-Partitionierungsschema* (*MBR – Master Boot Record*), das neuere (aber Microsoft-eigene) *Partitionierungsschema mit dynamischem Speicher* und das *GUID-Partitionsschema* (*GPT*, *GUID Partition Table*). (Ich werde alle drei nach dieser Einführung in eigenen Abschnitten ausführlich erläutern.) Microsoft bezeichnet eine Festplatte, die entweder das MBR- oder das GUID-Partitionierungsschema verwendet, als *Basisfestplatte* und ein Laufwerk, das das Partitionsschema mit dynamischem Speicher verwendet, als *dynamischen Datenträger*.

Ein einzelnes Windows-System mit drei Festplatten kann eines der Laufwerke mit MBR-Partitionsschema, ein zweites mit GPT-Partitionsschema und ein drittes als dynamischen Datenträger verwenden, und das System funktioniert perfekt. Was das bedeutet? Sie werden drei völlig unterschiedliche Arten der Partitionierung kennenlernen. Ich werde außerdem einige weitere Partitionstypen (z.B. verborgene Partitionen) erläutern und Ihnen zeigen, wann Sie selbst Partitionen anlegen können (und auch sollten).

9.1.1 Master Boot Record

Der erste Sektor einer MBR-Festplatte enthält den *Master Boot Record* (*MBR*). Genauer gesagt ist auf Festplatten, die das MBR-Partitionsschema verwenden, dort eine Datenstruktur gespeichert, die als Master Boot Record bezeichnet wird. Beim Systemstart durchsucht das BIOS den ersten Sektor des Startlaufwerks nach Befehlen. Zu diesem Zeitpunkt spielt es keine Rolle, welches Betriebssystem Sie verwenden oder wie viele Partitionen es gibt. Ohne die MBR-Datenstruktur wird Ihr Betriebssystem auch nicht geladen.

Hinweis

Eine Festplatte, die das MBR-Partitionierungsschema verwendet, wird von Technikern häufig kurz als *MBR-Laufwerk* bezeichnet. Ähnlich verhält es sich bei GPT-partitionierten Festplatten, die manche Techniker als *GPT-Laufwerke* bezeichnen.

Der MBR enthält außerdem die *Partitionstabelle*, die Informationen über die Anzahl und Größe der Partitionen auf dem Laufwerk liefert (Abbildung 9.5). Die MBR-Partitionstabelle unterstützt bis zu vier Partitionen – für mehr als das bietet die Partitionstabelle keinen Platz. Der Codeabschnitt im MBR hat nun die Aufgabe, in der Partitionstabelle nachzusehen, auf welcher Partition das derzeit gültige Betriebssystem gespeichert ist.

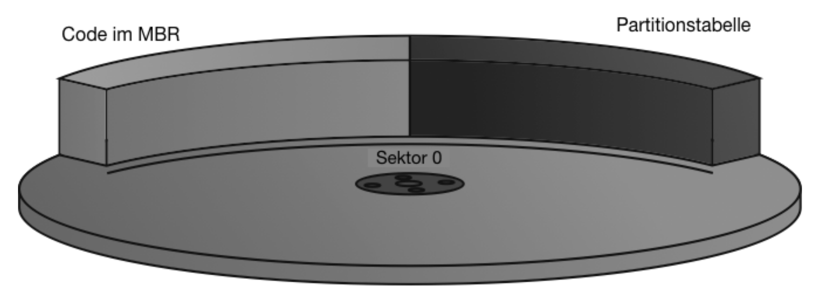


Abb. 9.5: Der Master Boot Record

Wenn der MBR die richtige Partition gefunden hat, übernimmt der sogenannte *Volume-Bootsektor* und lädt das Betriebssystem. Im Volume-Bootsektor sind wichtige Informationen über die Partition gespeichert, etwa wo genau auf der Partition sich die Bootdateien befinden (Abbildung 9.6).

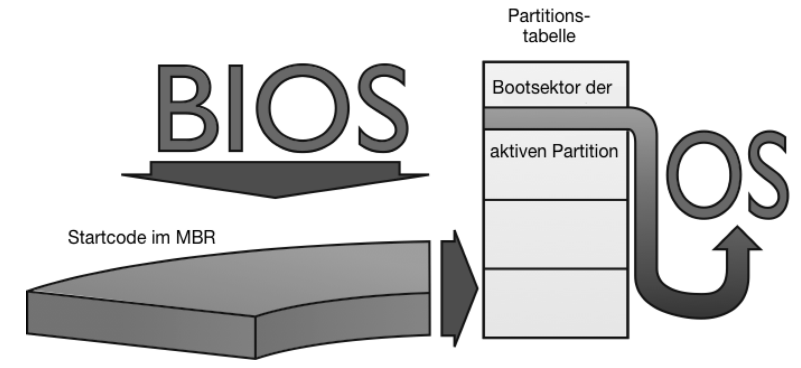


Abb. 9.6: Der MBR startet das Betriebssystem.

Wichtig

Pro MBR-Laufwerk gibt es nur einen MBR und eine Partitionstabelle. Jede Partition besitzt einen eigenen Volume-Bootsektor.

Die MBR-Partitionstabelle unterstützt zwei Partitionstypen, primäre und erweiterte Partitionen. *Primäre Partitionen* sollen bootfähige Betriebssysteme unterstützen. *Erweiterte Partitionen* sind nicht bootfähig. Eine einzige MBR-Festplatte kann bis zu drei primäre Partitionen und eine erweiterte Partition besitzen. Wird keine erweiterte Partition verwendet, können vier primäre Partitionen angelegt werden.

Primärpartitionen und mehrere Betriebssysteme

Primärpartitionen wird für gewöhnlich ein Laufwerksbuchstabe zugewiesen, unter dem sie dann im Explorer erscheinen, sobald sie formatiert sind. Der ersten primären Partitionen wird in Windows der Laufwerksbuchstabe `C:` zugewiesen. Danach können Sie weiteren Partitionen die Laufwerkbuchstaben `D:` bis `Z:` zuweisen.

Hinweis

Nicht jede Partition erhält notwendigerweise einen Laufwerksbuchstaben. Windows erstellt eine kleine Primärpartition namens »System-reserviert«, in der für den Systemstart wichtige Dateien gespeichert werden. Mehr dazu im Abschnitt *Bereitstellen von Laufwerken als Ordner*.

Die erste Primärpartition erhält übrigens den Namen `C:`, weil ältere PCs ein oder zwei Diskettenlaufwerke besaßen, die mit `A:` und `B:` bezeichnet wurden.

Ein Betriebssystem kann nur von einer Primärpartition gestartet werden. Auf einem MBR-Laufwerk lassen sich problemlos vier verschiedene Betriebssysteme installieren, jedes in seiner eigenen Primärpartition, und Sie können nach dem Einschalten des Computers auswählen, welches davon gestartet werden soll.

Für jede Primärpartition auf einem MBR-Laufwerk wird in der Partitionstabelle eine spezielle Einstellung gespeichert. Diese Einstellung gibt an, ob eine Primärpartition aktiviert oder deaktiviert ist. Beim Booten liest das BIOS bzw. der POST den MBR, um festzustellen, welche Primärpartition aktiviert ist.

Von dieser wird dann ein Betriebssystem geladen. Da jeweils nur ein Betriebssystem gestartet werden kann, ist auch nur jeweils eine Partition aktiv (Abbildung 9.7).

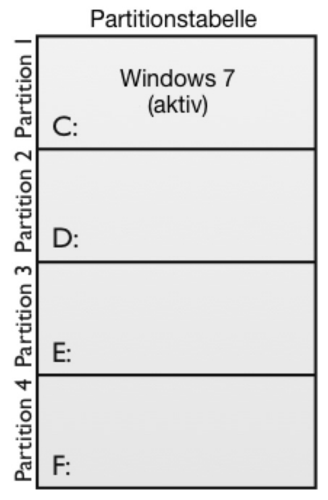


Abb. 9.7: Die aktive Partition enthält Windows 7

Um den Start mehrerer verschiedener Betriebssysteme zu ermöglichen, wird meist der kostenlose Linux-Boot-Manager namens *GRUB* (*Grand Unified Boot Manager*) verwendet, teilweise werden zu diesem Zweck aber auch andere Programme von Drittanbietern eingesetzt, wie z.B. der *Partition Commander* von Avanquest Software. Wenn der Computer startet, übernimmt GRUB die Kontrolle vom MBR und fragt, welches Betriebssystem gebootet werden soll (Abbildung 9.8). Sobald eine aktive Partition festgelegt ist, wird mittels des Volume-Bootsektors das Betriebssystem geladen.

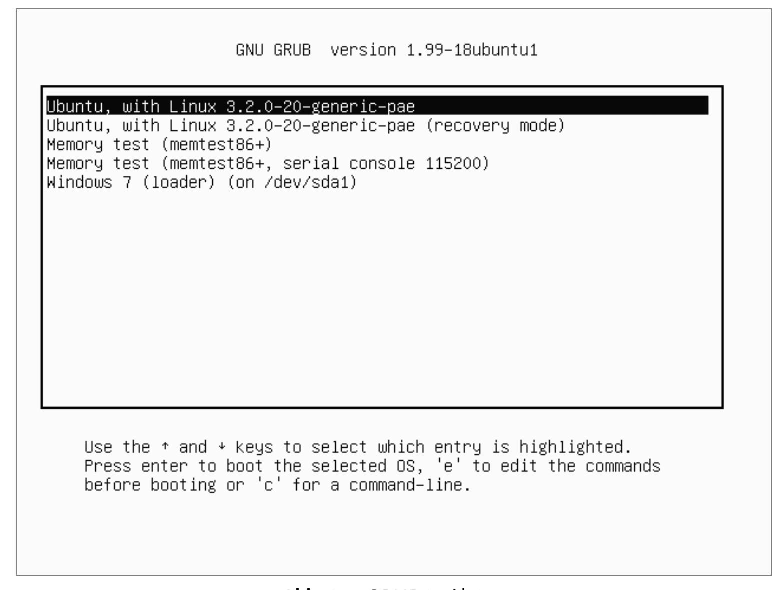


Abb. 9.8: GRUB in Aktion

Erweiterte Partitionen

Ein MBR-Laufwerk ist auf vier Partitionen beschränkt und Sie könnten nur vier Laufwerksbuchstaben benutzen, wenn Sie nur Primärpartitionen verwenden. Durch eine erweiterte Partition lässt sich das umgehen, denn Sie können *logische Laufwerke* innerhalb einer erweiterten Partition anlegen. Jedes logische Laufwerk erhält dann einen Laufwerksbuchstaben (Abbildung 9.9).

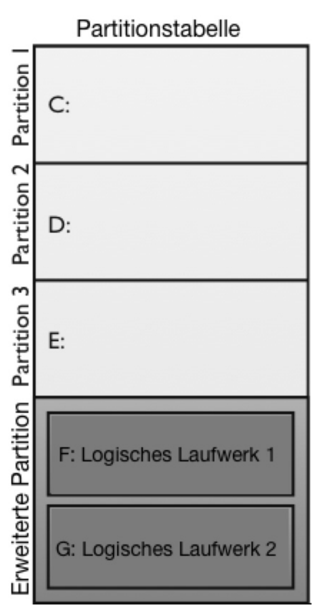


Abb. 9.9: Eine erweiterte Partition mit mehreren logischen Laufwerken

Ein logisches Laufwerk funktioniert wie eine Primärpartition und ihm wird normalerweise auch ein Laufwerksbuchstabe wie `D:` oder `E:` zugewiesen, aber Sie können kein Betriebssystem davon starten. Sie formatieren ein logisches Laufwerk wie eine Primärpartition. Der Unterschied besteht darin, dass jedes logische Laufwerk Teil derselben erweiterten Partition ist.

Wichtig

Erweiterte Partitionen erhalten *keinen* Laufwerksbuchstaben, nur die darauf befindlichen logischen Laufwerke.

9.1.2 Dynamische Datenträger

Mit Windows 2000 hat Microsoft mit den sogenannten *dynamischen Datenträgern* eine völlig neue Art der Partitionierung eingeführt. In diesem Zusammenhang wird anstelle des Begriffs *Partition* die Bezeichnung *Volume* verwendet. Bei dynamischen Datenträgern gibt es nichts mit primären und erweiterten Partitionen Vergleichbares. Ein Volume ist aus technischer Sicht zwar immer noch eine Partition, bietet aber Möglichkeiten, die über die regulärer Partitionen hinausgehen.

Hinweis

Die Begriffe »Partition« und »Volume« sind in diesem Zusammenhang gleichbedeutend. Sie verweisen auf einen bestimmten Teil der Festplatte.

Wenn Sie eine Festplatte als dynamischen Datenträger einrichten, können Sie darauf so viele Volumes anlegen, wie Sie möchten. Die Beschränkung auf vier Partitionen entfällt.

Sie können außerdem – durch Software – neue Laufwerksarten anlegen, die es bei MBR-Laufwerken nicht gibt, wie etwa RAID, übergreifende Datenträger und Volumes auf mehreren Laufwerken. Der Tabelle 9.1 können Sie entnehmen, welche Windows-Version welche Laufwerkstypen unterstützt.

Typ	Windows 7	Windows 8/8.1/10	Windows Server
Einfach	X	X	X
Übergreifend	X	X	X
Spripeset	X	X	X
Gespiegelt	X	X	X
RAID 5			X

Tabelle 9.1: Kompatibilität dynamischer Datenträger

Wichtig

Nur die Einsteigerversionen von Windows 7 unterstützen dynamische Datenträger nicht. Alle anderen Windows-Versionen, denen man heutzutage begegnet, unterstützen dagegen dynamische Datenträger.

Einfache Volumes verhalten sich ähnlich wie primäre Partitionen. Wenn die eine Hälfte einer Festplatte `E:`, die andere `F:` sein soll, legen Sie zwei Volumes auf einer dynamischen Festplatte an, das ist schon alles.

Übergreifende Volumes verwenden nicht zugewiesenen Speicherplatz auf mehreren Laufwerken, um ein einziges Volume zu bilden. Übergreifende Volumes sind etwas riskant – wenn eines der beteiligten Laufwerke ausfällt, ist das gesamte Volume dauerhaft verloren.

Stripesetvolumes sind RAID-0-Volumes. Sie können zwei beliebige nicht zugewiesene Speicherbereiche auf zwei separaten Festplatten nehmen und mit ihnen ein Stripesetvolume bilden. Aber auch hier verlieren Sie alle Daten, wenn eines der Laufwerke ausfällt.

Gespiegelte Volumes sind RAID-1-Volumes. Sie können zwei beliebige nicht zugewiesene Bereiche auf zwei separaten Festplatten nehmen und sie spiegeln. Fällt eines der beiden gespiegelten Laufwerke aus, läuft das andere weiter.

RAID-5-Volumes sind, wie der Name schon sagt, für RAID-5-Arrays vorgesehen. Ein RAID-5-Volume benötigt drei oder mehr dynamische Datenträger mit gleich großen, nicht zugewiesenen Speicherbereichen.

Hinweis

In Windows 8 und neueren Windows-Versionen gibt es ein RAID-System namens *Speicherplätze*, das sich von dynamischen Datenträgern unterscheidet. Mehr dazu im Abschnitt 9.3.5, *Speicherplätze*, weiter hinten in diesem Kapitel.

9.1.3 GUID-Partitionsschema

Das MBR-Partitionsschema wurde zu einer Zeit entwickelt, zu der man sich kaum vorstellen konnte, jemals mehr als 32 MB große Festplatten zu benötigen. Zwar war es seit sehr langer Zeit der Standard für die Partitionierung bootfähiger Laufwerke, aber es gibt nun einen Gegenspieler, der leistungsfähig genug ist, um das betagte MBR-Partitionsschema abzulösen.

Das *GUID-Partitionsschema* (*GPT*, Globally Unique Identifier Partition Table) hat vieles mit dem MBR-Partitionsschema gemeinsam, beseitigt aber die meisten von dessen Beschränkungen. Die wichtigsten Verbesserungen sind:

- MBR-Laufwerke sind auf vier Partitionen beschränkt. Bei einem GPT-Laufwerk ist hingegen eine nahezu unbegrenzte Zahl primärer Partitionen möglich. Microsoft hat Windows auf 128 Partitionen beschränkt.
- MBR-Partitionen dürfen nicht größer als 2,2 TB sein, während es bei GPT keine solche Grenze gibt. Es gibt zwar eine Grenze, aber die ist so groß, dass sie sich in Zettabyte bemisst. Ein Zettabyte entspricht übrigens rund einer Milliarde Terabyte.

Theoretisch ähnelt ein GPT-Laufwerk einem MBR-Laufwerk sehr, allerdings wird es durch LBA (*Logical Block Addressing*) unterteilt, nicht durch Sektoren (Abbildung 9.10). LBA 0 beispielsweise enthält den geschützten MBR. Hierbei handelt es sich um eine Kopie des Master Boot Records des MBR-Laufwerks, damit Festplattendienstprogramme erkennen können, dass es sich um ein GPT-Laufwerk handelt und nicht versehentlich irgendwelche Partitionierungsdaten überschreiben.

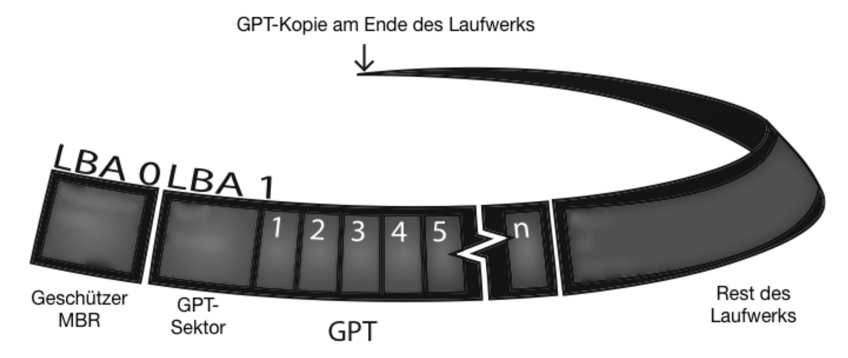


Abb. 9.10: GPTs müssen keine feste Größe besitzen

Anstelle des alten Master Boot Records und der Partitionstabelle tritt bei GPT ein Header (Vorspann) und eine Liste mit Einträgen für die verschiedenen Partitionen. Diese Daten befinden sich sowohl am Anfang als auch am Ende des Laufwerks, es gibt also eine Sicherheitskopie. Die Partitionen eines GPT-Laufwerks befinden sich zwischen dem primären Header nebst der Partitionsliste und deren Sicherheitskopien (Abbildung 9.10).

Die 64-Bit-Versionen der aktuellen Windows-Betriebssysteme können nur für den Start von einem GPT-Laufwerk konfiguriert werden, wenn Sie ein UEFI-Mainboard verwenden. Oder anders ausgedrückt: Wenn Sie versuchen, Windows 10 auf einem Rechner mit älterem Mainboard zu installieren, sind sie auf MBR angewiesen. Das Gleiche gilt für macOS. Die meisten Linux-Distributionen können sowohl mit dem älteren BIOS als auch mit UEFI-Firmware von GPT-Laufwerken booten.

Hinweis

Nun gut, wenn *GPT* also *GUID Partition Table* bedeutet, was bedeutet dann *GUID*? GUID steht für *Global Unique Identifier* und stellt eine Referenznummer für ein Objekt oder einen Vorgang dar, deren Wahrscheinlichkeit, doppelt vorzukommen, vernachlässigbar klein ist. Die Nummer ist somit für den fraglichen Vorgang oder das Objekt *eindeutig*.

9.1.4 Weitere Partitionstypen

Neben den von Windows unterstützten Partitionstypen gibt es noch einige andere. Zu den gebräuchlichsten gehört die *verborgene Partition*. Eine verborgene Partition ist eigentlich eine primäre Partition,

die vor Ihrem Betriebssystem verborgen ist. Nur spezielle BIOS-Programme können auf eine verborgene Partition zugreifen. Verborgene Partitionen werden von einigen PC-Herstellern zum Speichern einer Sicherungskopie eines installierten Betriebssystems verwendet. Auf diese können Sie zurückgreifen, um ein System wiederherzustellen, das versehentlich zerstört wurde, was z.B. passieren kann, wenn ein Partitionierungsprogramm fehlerhaft eingesetzt wird.

Wichtig

Verborgene Partitionen werden gelegentlich auch als *Recovery*-Partition bezeichnet.

Eine *Swap-Partition* (*Auslagerungspartition*) ist eine weitere spezielle Partition, die man jedoch nur auf Linux- und UNIX-Systemen findet. Eine Swap-Partition ist eine ganze Partition, die sich wie RAM verhält, wenn Ihr System mehr Arbeitsspeicher benötigt, als installiert ist. Die Aufgabe der Swap-Partition entspricht damit derjenigen der Auslagerungsdateien unter Windows, wie Sie aus Kapitel 4, *RAM*, bereits wissen.

9.1.5 Wann partitioniert werden sollte

Die Partitionierung ist keine alltägliche Aufgabe. Die beiden gebräuchlichsten Situationen, in denen Sie Festplatten wahrscheinlich partitionieren müssen, sind die Installation eines Betriebssystems auf einem neuen System und die zusätzliche Installation eines zweiten Festplattenlaufwerks. Wenn Sie ein neues Betriebssystem installieren, werden Sie bei der Installation irgendwann gefragt, wie das Laufwerk partitioniert werden soll. Wenn Sie zu einem vorhandenen System eine neue Festplatte hinzufügen, enthalten alle Betriebssysteme integrierte Werkzeuge, mit denen sie partitioniert werden kann.

Alle Windows-Versionen enthalten mehr oder weniger unterschiedliche Werkzeuge für die Partitionierung von Festplatten. Über 20 Jahre lang, während der Ära von DOS und des frühen Windows (bis Windows Me), benutzte man zum Partitionieren von Laufwerken ein Befehlszeilenprogramm namens `FDISK` (Abbildung 9.11). Neuere Windows-Versionen verwenden mit der DATENTRÄGERVERWALTUNG ein grafisches Partitionierungsprogramm (Abbildung 9.12), das Sie in der COMPUTERVERWALTUNG unter DATENSPEICHER finden. Darüber hinaus verfügt Windows über ein Kommandozeilenprogramm zur Datenträgerverwaltung namens `diskpart`, das in Kapitel 16, *Fehlerbehebung*, ausführlich erläutert wird.

```
                    Microsoft Windows 98
              Festplatten-Konfigurationsprogramm
          (C)Copyright Microsoft Corp. 1983 - 1998

                        FDISK-Optionen

Aktuelle Festplatte: 1

Wählen Sie eine der folgenden Optionen:

1. DOS-Partition oder logisches DOS-Laufwerk erstellen
2. Aktive Partition festlegen
3. Partition oder logisches DOS-Laufwerk löschen
4. Partitionierungsdaten anzeigen


Optionsnummer eingeben: [1]




FDISK beenden mit ESC
```

Abb. 9.11: FDISK

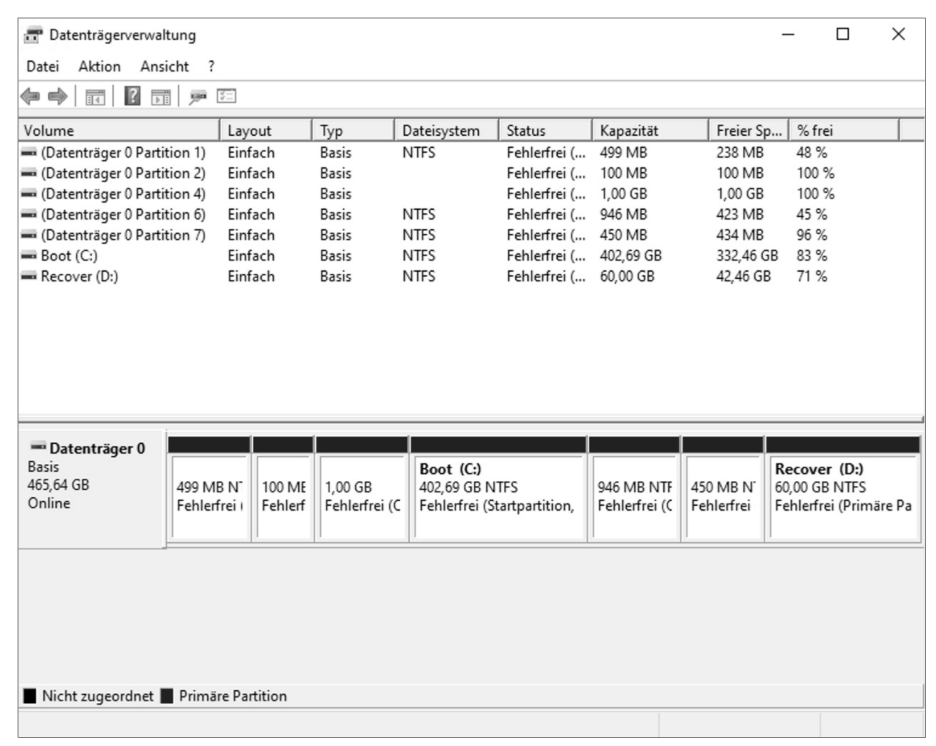


Abb. 9.12: Die DATENTRÄGERVERWALTUNG in der COMPUTERVERWALTUNG unter Windows 10

Linux verwendet verschiedene andere Werkzeuge für die Partitionierung. Das älteste heißt FDISK, genau wie die DOS/Windows-Version. Das ist allerdings die einzige Gemeinsamkeit, denn das Linux-FDISK verwendet einen ganz anderen Befehlssatz. Auch wenn in jeder Linux-Version FDISK enthalten ist, wird es selten verwendet, weil es sehr viel bessere Werkzeuge für die Partitionierung gibt. Eines der neuen entsprechenden Werkzeuge unter Linux heißt *GParted*. Im Abschnitt *Jenseits von A+* werden einige Werkzeuge zum Partitionieren von Drittanbietern vorgestellt.

In den Anfangszeiten des PCs ließ sich Art oder Größe einer einmal angelegten Partition mit Bordmitteln nicht mehr ändern, sofern sie nicht komplett gelöscht wird. Mit Werkzeugen von Drittanbietern, allen voran *PartitionMagic*, konnten Techniker die Größe von Partitionen ändern, ohne die darin enthaltenen Daten zu verlieren. Die aktuellen Werkzeuge von Microsoft sind in dieser Hinsicht flexibler. Unter Windows können Sie die Partitionsgrößen beliebig und verlustfrei ändern (sofern freie Bereiche vorhanden sind).

Tipp

Sehen Sie sich die Übung zum Ändern der Größe einer Partition unter `http://totalsem.com/100x` an! Sie finden dort weitere wertvolle Tipps für die Prüfung.

9.1.6 Begriffsverwirrung

Bislang hieß es immer, dass MBR- und GPT-Festplatten *Partitionen* und dynamische Datenträger *Volumes* verwenden. Leider zeigt das entsprechende Werkzeug (DATENTRÄGERVERWALTUNG) in neueren Windows-Versionen (8/8.1/10) nur noch an, dass Sie im Begriff sind, ein *Volume* anzulegen (Abbildung 9.13).

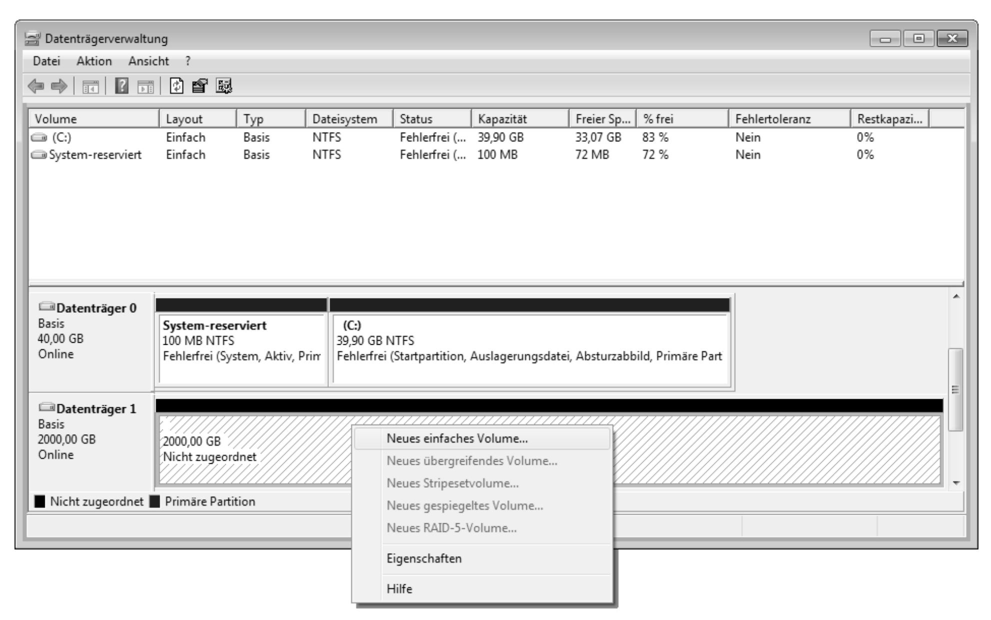


Abb. 9.13: Im Kontextmenü ist nur von Volume die Rede, nicht von Partitionen.

Obwohl im Kontextmenü von einem *Volume* die Rede ist, erstellen Sie eine *Partition* auf einer Basisfestplatte. Abbildung 9.14 zeigt die Datenträgerverwaltung in Windows 8.1 mit einer partitionierten Basisfestplatte. Dabei handelt es sich um zwei primäre Partitionen.

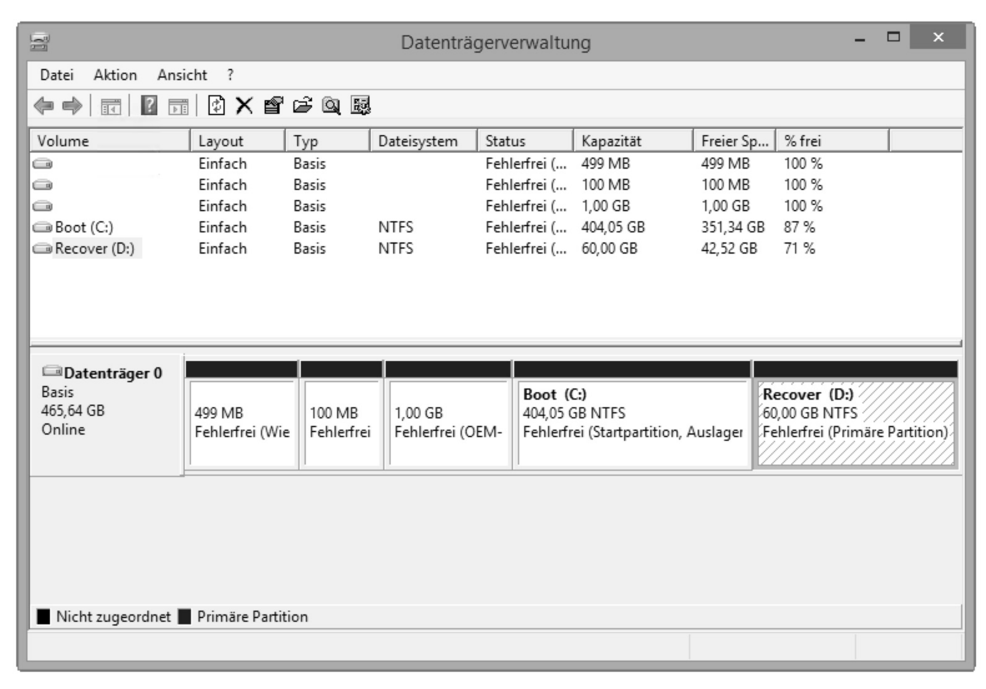


Abb. 9.14: Festplatte mit zwei Partitionen in der DATENTRÄGERVERWALTUNG von Windows 8

9.2 Formatierung von Festplatten

Nach der Partitionierung der Festplatte besteht die Partition lediglich aus einer großen Anzahl von Blöcken. Das Betriebssystem muss Dateien mit Namen wie `Urlaubserinnerungen.mp4` oder `chrome.exe` speichern können. Deshalb müssen all diese Blöcke organisiert werden (Abbildung 9.15).

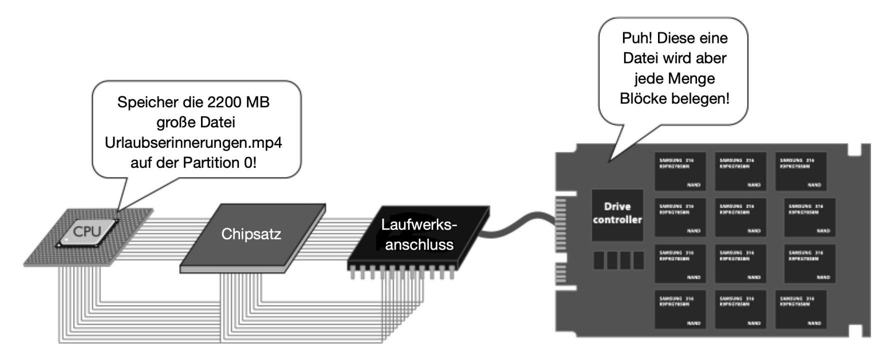


Abb. 9.15: Große Dateien erfordern viele Blöcke.

Durch die *Formatierung* wird ein Dateisystem erzeugt, das all die zur Partition gehörenden Blöcke organisiert und es ermöglicht, Dateien zu speichern und abzurufen. Zudem wird ein *Haupt-* oder *Stammverzeichnis* für das Dateisystem angelegt, damit die Partition Ordner speichern kann. Alle einzurichtenden Partitionen und Datenträger müssen formatiert werden, damit Daten so auf ihnen gespeichert werden können, dass sie sich leicht wiederfinden lassen.

Alle Betriebssysteme verwenden ihr eigenes Dateisystem. Was Apple-Anwender betrifft: macOS verwendet Dateisysteme, die APFS und HFS+ heißen. Linux-Anwendern steht eine große Auswahl zur Verfügung; die meisten verwenden ext4, aber es gibt viele andere, die Bezeichnungen wie BTRFS, XFS, ZFS etc. tragen. Windows verwendet Dateisysteme, die NTFS, FAT32 und exFAT heißen. Wir werden zunächst einmal betrachten, was ein Dateisystem eigentlich leistet (am Beispiel von Windows). Dann sehen wir uns die Unterschiede an.

Hinweis

Ein bestimmtes Betriebssystem kann in der Lage sein, das Dateisystem eines anderen Betriebssystems zu lesen – oder auch nicht. Die meisten Linux-Systeme können beispielsweise problemlos das NTFS-Dateisystem von Windows lesen.

9.2.1 Dateisysteme unter Windows

Alle Windows-Versionen enthalten ein Formatierungsprogramm, mit dem Sie eines der unterstützten Dateisysteme auf einer Partition oder einem Volume erstellen können. Die aktuellen Windows-Versionen unterstützen drei Microsoft-Dateisysteme: FAT32, NTFS und exFAT (für Wechseldatenträger). Alle Windows-Dateisysteme organisieren Datenblöcke in Form von Gruppen, die als *Cluster* bezeichnet werden. Die Größe eines Clusters ist vom Dateisystem und der Partitionsgröße abhängig. Windows verwendet Cluster, um einige der Beschränkungen bei der Adressierung zu umgehen, die den Dateisystemen zu eigen sind. (Ich habe für die verschiedenen Dateisysteme Diagramme erstellt, die zeigen, wie die Cluster skalieren.)

Das einfachste Dateisystem für Festplatten wird FAT oder FAT16 genannt und eignet sich bereits gut zur Darstellung der Arbeitsweise aller Dateisysteme, weshalb ich mit ihm beginnen werde. Komplexere Dateisysteme beheben viele der dem FAT-Dateisystem innewohnenden Probleme und bieten zudem zusätzliche Funktionen.

9.2.2 FAT32

Die grundlegende Speichereinheit einer Festplatte ist ein Block, der bis zu 4096 Byte Daten speichern kann. Bei einer kleinen Partition besteht jeder Cluster aus einem Block. Ist eine Datei größer als 4096 Byte, werden so viele Cluster verwendet, wie zum Speichern der Datei notwendig ist. Das Betriebssystem muss über eine Methode verfügen, mit der es in einen Cluster schreiben, einen unbenutzten finden, wiederum schreiben und damit fortfahren kann, bis die Datei komplett gespeichert ist. Wenn das Betriebssystem die Datei gespeichert hat, muss es anschließend weiterhin wissen, in welchem Cluster sich diese befindet, um sie später wieder lesen zu können. Wenn ein Betriebssystem eine Datei, die kleiner als 4096 Byte ist, in einem Cluster speichert, wird der restliche Platz verschwendet. Diese Platzverschwendung ist tolerierbar, da die meisten Dateien weit größer als 4096 Byte sind.

Die MS-DOS-Version 2.1 unterstützte erstmals Festplatten unter Verwendung einer speziellen Datenstruktur, die die auf einer Festplatte gespeicherten Daten aufzeichnen konnte. Microsoft nannte diese Datenstruktur *FAT* (*File Allocation Table*, Dateizuordnungstabelle). Die Dateizuordnungstabelle können Sie sich wie einen Karteikasten vorstellen, in dem protokolliert wird, welche Cluster die verschiedenen Teile einer Datei speichern. Offiziell wird die Dateizuordnungstabelle zwar als *Datenstruktur* bezeichnet, man kann sie sich aber besser als zweispaltige Tabelle vorstellen.

Die linke Spalte der Tabelle (siehe Abbildung 9.16) enthält für jeden Cluster eine hexadezimale Nummer, und zwar zwischen 00000000 und FFFFFFFF. Jedes Hexadezimalzeichen steht für vier binäre Werte bzw. vier Bit. Acht Hexadezimalziffern repräsentieren daher 32 Bit. Es gibt also 2^{32} Cluster, die indiziert werden können. Das sind etwas mehr als vier Milliarden.

LBA-Nummer	Status
00000000	
00000001	
00000002	
00000003	
00000004	
00000005	
FFFFFFFA	
FFFFFFFB	
FFFFFFFC	
FFFFFFFD	
FFFFFFFE	
FFFFFFFF	

Abb. 9.16: 32-Bit-FAT

Hinweis

Einstellige Hexadezimalzahlen decken den Bereich der Dezimalzahlen 0 bis 15 ab und man verwendet zu ihrer Darstellung die Ziffern 0 bis 9 sowie die Buchstaben A bis F. Jede Hexadezimalstelle repräsentiert 4 Binärzahlen oder Bits. Um den Wert zu berechnen, werden sie summiert. Die Binärzahl 0000 entspricht also der Hexadezimalzahl 0. Wenn man die Binärzahl hochzählt, ergibt sich 0001, was als Hexadezimalzahl ebenfalls als 1 geschrieben wird. Interessant wird es, wenn man die Dezimalzahl 10 erreicht. Binär schreibt man 1010, aber da im Hexadezimalsystem nur eine Stelle für Zahlen kleiner als 16 verwendet wird, schreibt man hierfür A. B steht für die Dezimalzahl 11 bzw. die Binärzahl 1011 usw.

Diese Art der FAT wird *32-Bit-FAT* oder kurz *FAT32* genannt. Nicht nur Festplatten und SSDs nutzen FATs. Viele USB-Sticks verwenden ebenfalls FAT32.

Die rechte Spalte der FAT enthält Daten über den Clusterstatus. Alle Festplatten, sogar die brandneuen, die direkt aus der Fabrik kommen, enthalten fehlerhafte Blöcke, die wegen Unvollkommenheiten bei der Fertigung der Festplatte keine Daten mehr speichern können. Das Betriebssystem muss diese defekten Blöcke lokalisieren, als unbrauchbar markieren und anschließend dauerhaft verhindern, dass an diese Stellen Dateien geschrieben werden. Eine der Funktionen der sogenannten *Highlevel-Formatierung* besteht in dieser Kartierung defekter Sektoren. Nachdem das Formatierungsprogramm die FAT erstellt hat, überprüft es die gesamte Partition und versucht, jeden Block sequenziell zu beschreiben und zu lesen. Wenn es einen defekten Block findet, markiert es diesen in der FAT mit einem speziellen Code (0000FFF7), der anzeigt, dass dieser Cluster nicht verwendet werden kann. Auch brauchbare Blöcke werden bei der Formatierung gekennzeichnet, und zwar mit dem Code 00000000 (Abbildung 9.17).

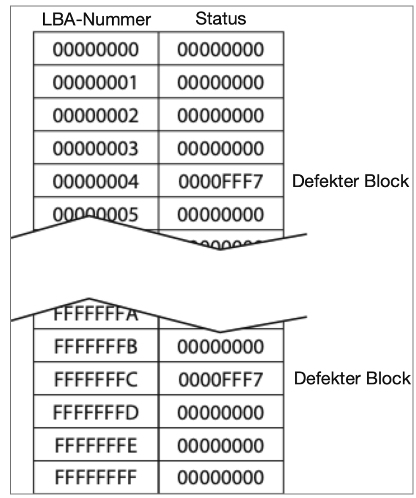


Abb. 9.17: Gekennzeichnete defekte Blöcke

Hinweis

Bei der Highlevel-Formatierung werden wie erwähnt die FAT und ein leeres Stammverzeichnis erstellt. Verzichtet man auf die Überprüfung der Sektoren, bezeichnet Microsoft diesen Vorgang als *Schnellformatierung*. Alternativ können Sie das Formatierungsprogramm auch veranlassen, alle Blöcke zu überprüfen, um die unbrauchbaren in der FAT zu kennzeichnen. Hierbei handelt es sich um eine vollständige Formatierung.

FAT32 in Aktion

Nehmen Sie einmal an, dass Sie Windows mit FAT32 nutzen. Wenn eine Anwendung wie etwa Microsoft Word das Betriebssystem zum Speichern einer Datei auffordert, sucht Windows ab dem Anfang der FAT nach dem ersten freien Cluster-Eintrag (00000000) und beginnt dort mit dem Schreiben. Wenn die Datei komplett in diesen Cluster passt, trägt Windows in das Statusfeld des Clusters in der FAT den Code »0000FFFF« (letzter Cluster) ein. Dieser dient zur Markierung des Dateiendes (*EOF – End Of File*). Anschließend sucht Windows dann den Ordner auf, in dem die Datei gespeichert ist, und schreibt dort den Dateinamen und die Nummer des Clusters in die Ordnerliste. Falls die Datei mehr als einen Cluster beansprucht, sucht Windows nach dem nächsten freien Cluster und trägt dessen

Nummer ins Statusfeld ein. Dieser Vorgang wird wiederholt, bis die Datei komplett gespeichert ist. Beim letzten Cluster wird im Statusfeld der Dateiende-Code »0000FFFF« eingetragen.

Das folgende Beispiel soll diese Vorgehensweise verdeutlichen. Nehmen Sie an, dass Sie in einen Bereich in der FAT zwischen 03213ABB bis 03213AC7 schreiben, und nehmen Sie weiter an, dass Sie die Datei `mom.txt` speichern möchten. Die FAT sieht vor dem Speichern dieser Datei wie in Abbildung 9.18 aus.

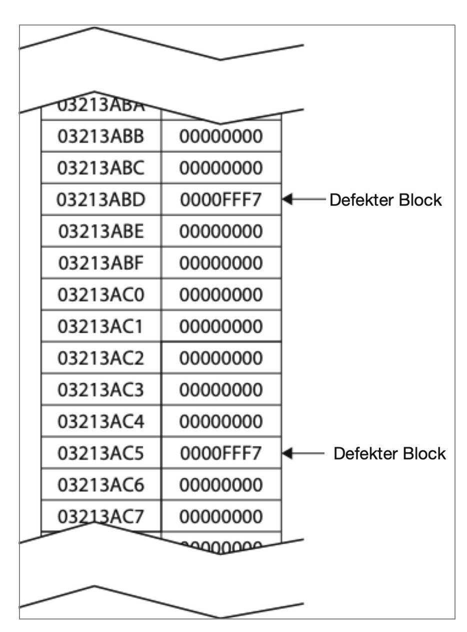


Abb. 9.18: Der Ausgangszustand der FAT

Windows findet den ersten freien Cluster 03213ABB und speichert in ihm Daten. Da der Inhalt von `mom.txt` nur teilweise in diesen Cluster passt, sucht das Betriebssystem in der FAT nach einem weiteren freien Cluster. Bevor es in den gefundenen Cluster 03213ABC schreibt, wird im Statusfeld von 03213ABB der Wert 03213ABC eingetragen.

Auch nach dem Schreiben zweier Cluster ist die Datei `mom.txt` noch nicht vollständig gespeichert, sodass Windows einen weiteren freien Cluster aufspüren muss. Der Cluster 03213ABD wurde als defekt (0000FFF7) markiert und wird daher übergangen. Windows findet daraufhin den Cluster 00003ABE.

Bevor Windows Daten in den Cluster 03213ABE schreibt, trägt es in das Statusfeld von 03213ABC den Wert 03213ABE ein. Windows benötigt nicht den ganzen Cluster 03213ABE, da die Datei `mom.txt` nun komplett gespeichert werden konnte. Daher trägt Windows in das Feld 03213ABE den Wert 0000FFFF ein, der das Dateiende markiert (Abbildung 9.19).

Nach dem Schreiben der Cluster sucht Windows nach dem Ordner für die Datei. (Auch Ordner werden in Clustern gespeichert. Sie belegen jedoch andere Gruppen von Clustern an anderer Position auf der Festplatte.) Im Ordner zeichnet Windows den Dateinamen, die Größe, das Datum, die Uhrzeit und den Start-Cluster wie folgt auf:

```
mom.txt 13234 05-19-19 2:04p 03213ABB
```

Wenn nun ein Programm auf diese Datei zugreifen will, wird der beschriebene Prozess umgekehrt. Windows sucht nach dem Ordner, der die Datei enthält, und ermittelt den Start-Cluster. Anschließend

kopiert es so lange die Daten der zusammenhängenden Cluster, bis es auf das Zeichen für das Dateiende stößt. Anschließend übergibt Windows die auf diese Weise zusammengesetzte Datei der Anwendung, die sie angefordert hat.

Ohne Dateizuordnungstabelle kann Windows Dateien offensichtlich nicht wiederfinden. Beim FAT32-Dateisystem werden automatisch zwei Kopien der FAT erstellt, damit eine Sicherheitskopie vorhanden ist, mittels derer die ursprüngliche FAT im Falle einer Beschädigung (die leider recht häufig vorkommt) wiederhergestellt werden kann.

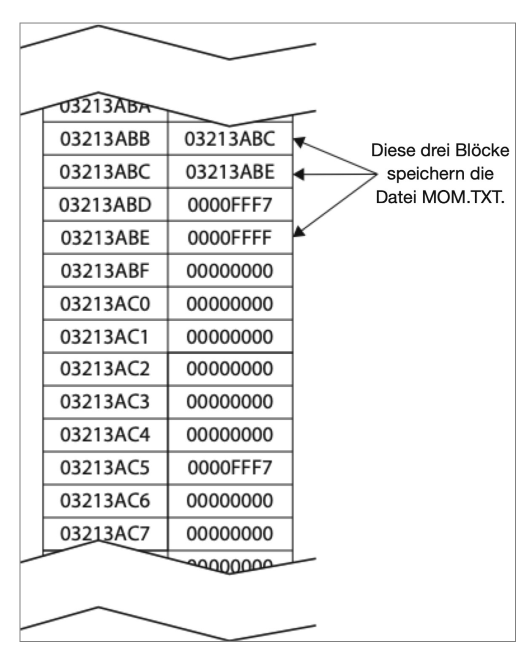


Abb. 9.19: Das Dateiende ist erreicht.

Clustergrößen bei FAT32

Die Clustergröße hängt vom Dateisystem ab. FAT32 bietet 4-KB-Clustergrößen (4 KB große Blöcke) bis zu einer Partitionsgröße von 2 GB. Für größere Partitionen sind mehr Blocks pro Cluster erforderlich, was die Effizienz des Laufwerks etwas verringert. Tabelle 9.2 zeigt die Clustergrößen bei FAT32-Partitionen.

Laufwerksgröße	Clustergröße
512 MB bis 1023 MB	4 KB
1024 MB bis 2 GB	4 KB
2 GB bis 8 GB	4 KB
8 GB bis 16 GB	8 KB
16 GB bis 32 GB	16 KB
> 32 GB	32 KB

Tabelle 9.2: FAT32-Clustergrößen

FAT32 ist auch heutzutage noch gebräuchlich, allerdings nicht für Partitionen, auf denen ein Betriebssystem installiert ist, sondern vornehmlich bei kleineren (< 32 GB) USB-Speichersticks.

Fragmentierung

Nehmen Sie nun in Fortsetzung des letzten Beispiels an, dass zwei weitere Dateien mit Microsoft Word gespeichert werden: zwei Briefe namens `Wichtiges Dokument 31.docx` und `Systemspeicher.docx`. Die Datei `Wichtiges Dokument 31.docx` beansprucht die nächsten drei Cluster 03213ABF, 03213AC0 und 03213AC1, während `Systemspeicher.docx` zwei Cluster belegt, nämlich 03213AC2 und 03213AC3 (Abbildung 9.20).

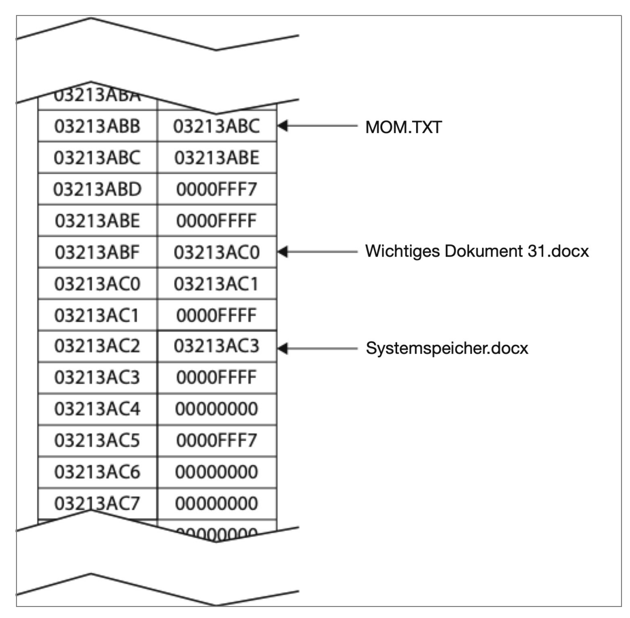


Abb. 9.20: Drei gespeicherte Dateien

Wenn wir annehmen, dass sich diese drei Dateien im selben Ordner befinden, sehen die Dateiinformationen folgendermaßen aus:

```
mom.txt                       13234 05-19-20 2:04p 03213ABB
Wichtiges Dokument 31.docx     9276 05-19-20 2:07p 03213ABF
Systemspeicher.docx            5434 05-19-20 2:10p 03213AC2
```

Als Nächstes wird `mom.txt` gelöscht. Beim Löschen einer Datei entfernt Windows nicht die Block-Einträge, sondern ändert lediglich die Informationen im Ordner, indem es – hier im Beispiel – den ersten Buchstaben des Dateinamens `mom.txt` durch den griechischen Kleinbuchstaben Sigma (σ) ersetzt. Soweit es das Betriebssystem betrifft, ist die Datei damit »verschwunden«. Sie wird im Windows-Explorer nicht mehr angezeigt, obwohl die Daten sich noch immer auf der Festplatte befinden.

```
σom.txt                       13234 05-19-20 2:04p 03213ABB
```

Beachten Sie, dass Windows unter normalen Umständen Dateien tatsächlich gar nicht löscht, wenn Sie die `Entf`-Taste drücken. Stattdessen verschiebt Windows die Dateiinformationen (aber nicht die Blöcke selbst) in ein spezielles verborgenes Verzeichnis, auf das Sie über den Papierkorb Zugriff haben. Die eigentlichen Dateien werden nicht gelöscht, bis Sie den Papierkorb leeren.

Da also alle Daten von `mom.txt` noch intakt sind, könnten Sie nun spezielle Programme verwenden, die das σ wieder in einen anderen Buchstaben zurückverwandeln und das Dokument so wieder ver-

fügbar machen. Es gibt zahlreiche Werkzeuge von Drittanbietern, die das Löschen rückgängig machen können. Abbildung 9.21 zeigt ein solches Programm bei der Arbeit. Beachten Sie, dass Sie ein Werkzeug zum Rückgängigmachen des Löschens möglichst schnell nach dem Löschen ausführen müssen. Der Platz, der Ihrer gelöschten Datei zugewiesen war, kann schon bald mit einer neuen Datei überschrieben werden.

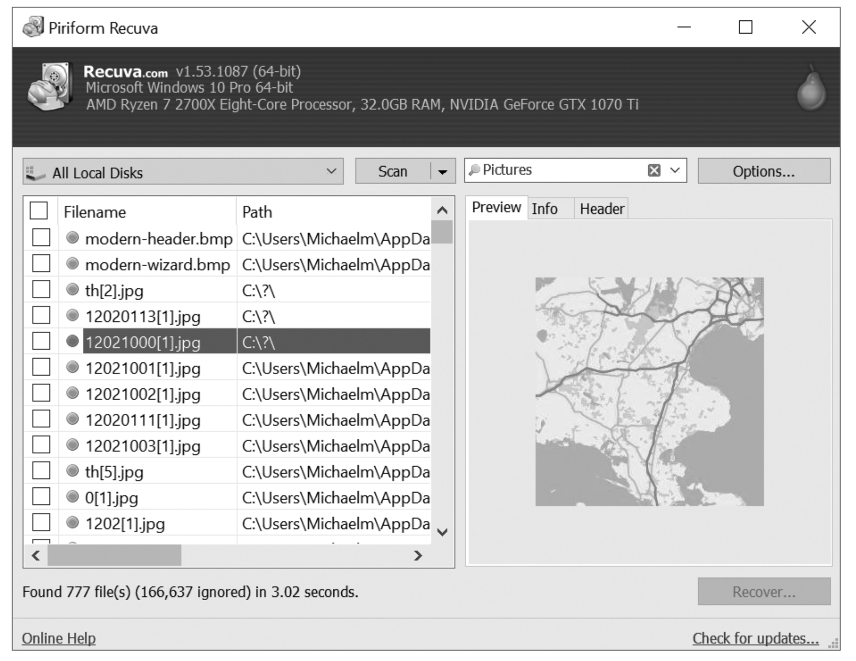


Abb. 9.21: Piriform Recuva bei der Arbeit

Wichtig

Möglicherweise werden Sie in der Prüfung danach gefragt, wie man eine gelöschte Datei wiederherstellen kann. Falls sie sich noch im Papierkorb befindet, brauchen Sie ihn nur zu öffnen, mit der rechten Maustaste auf die Datei zu klicken und WIEDERHERSTELLEN auszuwählen. Falls die Datei unter Umgehung des Papierkorbs gelöscht wurde oder aus einem anderen Grund nicht mehr vorhanden ist, müssen Sie sich nach einer Software eines Drittherstellers umsehen, da Microsoft kein Werkzeug zum Wiederherstellen gelöschter Dateien anbietet.

Nehmen Sie einmal an, dass Sie als Nächstes den Papierkorb leeren. Jetzt speichern Sie in demselben Ordner, in dem sich bereits `mom.txt` befand, eine Datei namens `Steuern.xls`, die eine große Tabelle enthält und sechs Cluster beansprucht. Beim Schreiben dieser Datei auf die Festplatte überschreibt Windows den Speicherplatz, der ursprünglich von `mom.txt` belegt wurde, und benutzt noch drei weitere Cluster. Die nächsten drei verfügbaren Cluster sind jetzt 03213AC4, 03213AC5 und 03213AC6 (Abbildung 9.22).

Beachten Sie, dass `Steuern.xls` nun in zwei Teile aufgeteilt und damit »fragmentiert« ist. Im Beispiel wurde die Datei nur in zwei fragmentierte Teile zerlegt, in der Praxis können Dateien aber aus Hunderten von Fragmenten bestehen, sodass die Schreib/Leseköpfe der Festplatte beim Lesen der Datei über die gesamte Festplatte bewegt werden müssen. Wenn Dateien nicht fragmentiert sind, können sie deshalb deutlich schneller von der Festplatte gelesen werden.

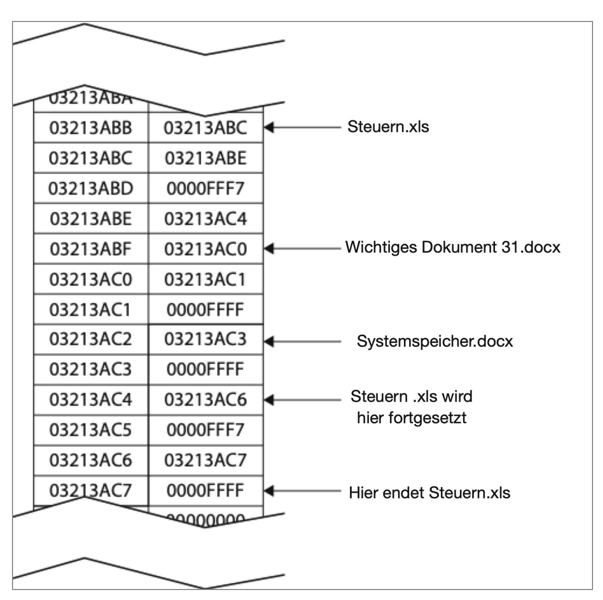


Abb. 9.22: Die fragmentierte Datei `Steuern.xls`

Alle modernen Windows-Versionen enthalten ein Defragmentierungsprogramm (Abbildung 9.23), das fragmentierte Dateien neu anordnet und in benachbarten, zusammenhängenden Bereichen ablegt (DEFRAGMENTIERUNG unter Windows 7 bzw. LAUFWERKE OPTIMIEREN unter Windows 8/8.1/10). Windows führt sie standardmäßig automatisch aus. Die *Defragmentierung* hat entscheidenden Einfluss auf die Arbeitsgeschwindigkeit mechanischer Festplatten. In Abschnitt 9.4, *Wartung und Fehlerbehebung bei Festplatten*, erfahren Sie mehr über den Einsatz der verschiedenen Windows-Defragmentierungsprogramme.

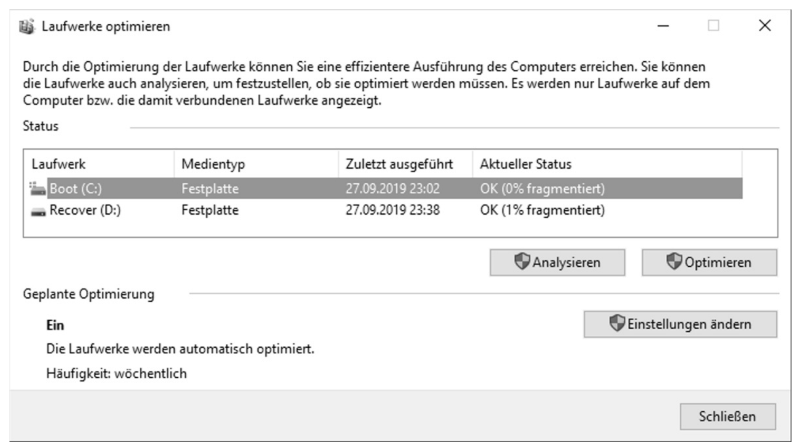


Abb. 9.23: Laufwerke optimieren unter Windows 10

Bei SSDs gibt es ebenfalls eine Fragmentierung, aber dank der Eigenschaften einer SSD kann auf jede Speicherseite fast gleich schnell zugegriffen werden. Bei der ersten SSD-Generation verblieben die einmal in eine Speicherzelle geschriebenen Daten dort, bis das Laufwerk fast voll war. Auch wenn sie Daten einer gelöschten Datei enthielt, wurde die Zelle nicht sofort gelöscht oder überschrieben, weil

der SSD-Controller nicht feststellen konnte, ob der Speicherinhalt seitens des Betriebssystems gelöscht worden war. Da die Speicherzellen einer SSD nur eine begrenzte Anzahl von Schreibvorgängen überstehen, bis sie »verschlissen« sind, warteten die SSDs der ersten Generation mit dem Löschen und erneuten Beschreiben einer Zelle, bis alle Zellen der SSD beschrieben waren.

Moderne SSDs verfügen über ein Feature namens *Trim*, das es dem Betriebssystem ermöglicht, Kommandos zum Aufräumen und Wiederverwenden gelöschter Speicherbereiche abzusetzen. Das geschieht automatisch, deshalb gibt es keinerlei Grund, eine SSD zu defragmentieren.

9.2.3 NTFS

Das Format der Wahl unter Windows ist heute *NTFS* (*New Technology File System*). NTFS wurde vor langer Zeit zusammen mit der ersten Version von Windows NT veröffentlicht, daher auch der Name. Im Laufe der Jahre wurden zahlreiche Verbesserungen an NTFS vorgenommen. NTFS verwendet ebenfalls Cluster und Dateizuordnungstabellen (*File Allocation Tables*), die aber viel komplexer und leistungsfähiger als bei FAT32 sind. NTFS bietet sechs wesentliche Verbesserungen und Optimierungen: Redundanz, Sicherheit, Komprimierung, Verschlüsselung, Kontingente und variable Clustergrößen.

Hinweis

Wenn Sie unbedingt wissen wollen, welche NTFS-Version Ihr System verwendet, dann geben Sie an der Eingabeaufforderung den Befehl `fsutil fsinfo ntfsinfo c:` ein.

NTFS-Struktur

NTFS verwendet eine verbesserte Dateizuordnungstabelle, die sogenannte *MFT* (*Master File Table*). Eine NTFS-Partition bewahrt eine Sicherungskopie der wichtigsten Teile der MFT in der Mitte der Festplatte auf, womit die Wahrscheinlichkeit reduziert wird, dass ernsthafte Festplattenfehler sowohl die MFT als auch die MFT-Kopie löschen.

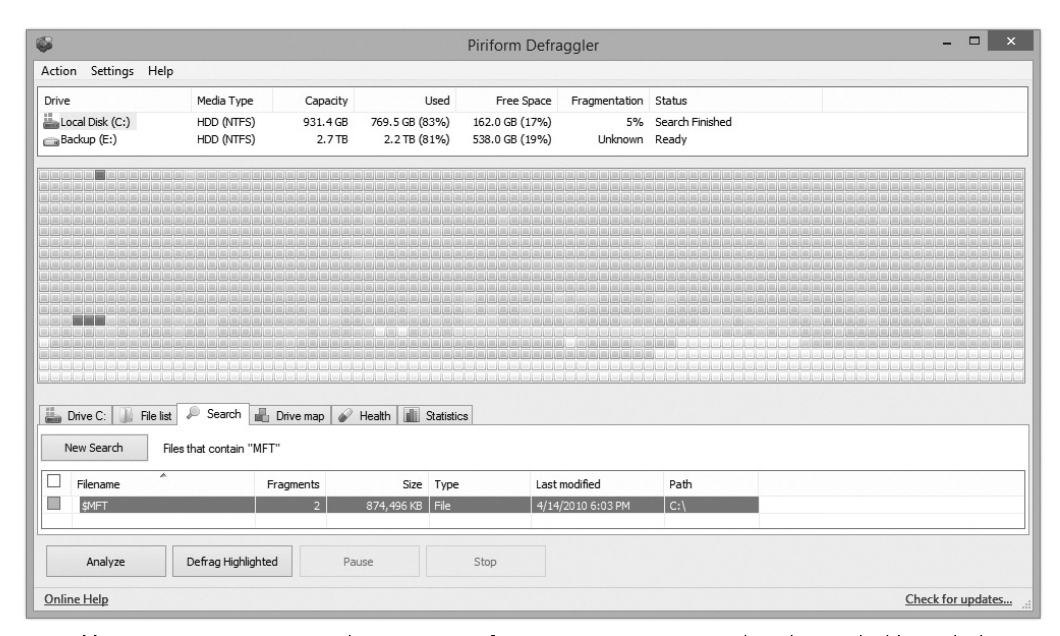


Abb. 9.24: Die NTFS-MFTs werden in einem Defragmentierungsprogramm als nicht verschiebbare Blöcke gekennzeichnet.

Immer, wenn Sie eine NTFS-Partition defragmentieren, sehen Sie einen kleinen, nicht verschiebbaren Bereich irgendwo auf dem Laufwerk, meist in der Nähe des Anfangs, bei dem es sich um die Sicherung der MFT handelt (Abbildung 9.24). (Diese ist allerdings bei großen Festplatten oft derart winzig, dass sie kaum mehr sichtbar ist.)

Sicherheit

NTFS betrachtet einzelne Dateien und Ordner als Objekte und sorgt über die sogenannte *Zugriffssteuerungsliste* bzw. *ACL* (*Access Control List*) für die Sicherheit dieser Objekte. Weitere der folgenden Kapitel werden genauer darauf eingehen.

Hinweis

Die genaue Funktionsweise von NTFS wurde von Microsoft nie veröffentlicht.

Komprimierung

Mit NTFS können Sie einzelne Dateien und Ordner komprimieren, um Platz auf einer Festplatte zu sparen. Die Komprimierung verlangsamt den Zugriff auf die Daten, weil das Betriebssystem die Dateien jeweils dekomprimieren muss, aber bei Speicherplatzproblemen bleibt einem manchmal keine andere Alternative. Die Namen komprimierter Dateien werden im Explorer blau dargestellt.

Hinweis

Unter bestimmten Umständen kann die Komprimierung den Zugriff beschleunigen, nämlich wenn die CPU die Dekomprimierung schneller vornimmt, als das Laufwerk Daten liefert. Bei komprimierten Dateien muss das Laufwerk weniger Daten senden, und die CPU kann sie entgegennehmen und im Arbeitsspeicher dekomprimieren.

Verschlüsselung

Einer der großen Vorteile von NTFS ist die Dateiverschlüsselung, die Schwarze Kunst, Dateien für all diejenigen unlesbar zu machen, die nicht den richtigen Schlüssel besitzen. Sie können eine einzelne Datei, einen Ordner oder einen ganzen Ordner mit Dateien verschlüsseln. Microsoft bezeichnet das Verschlüsselungswerkzeug in NTFS als *EFS* (*Encrypting File System*), aber es handelt sich dabei nur um einen Aspekt von NTFS, nicht um ein eigenständiges Dateisystem. In Kapitel 13 erfahren Sie mehr über Verschlüsselung.

Datenträgerkontingente

NTFS unterstützt Datenträgerkontingente, sodass Administratoren Obergrenzen für den für einzelne Benutzer verfügbaren Speicherplatz auf einem Laufwerk vorgeben können. Um Kontingente einzurichten, müssen Sie sich als Administrator anmelden. Klicken Sie mit der rechten Maustaste den Festplattennamen an und wählen Sie EIGENSCHAFTEN.

Im Dialogfeld EIGENSCHAFTEN VON LAUFWERK nehmen Sie auf der Registerkarte KONTINGENT geeignete Einstellungen vor. Abbildung 9.25 zeigt die für eine Festplatte konfigurierten Kontingente. Auf Einzelbenutzersystemen findet man solche Einstellungen selten, aber auf Mehrbenutzersystemen verhindern sie, dass ein Benutzer den gesamten Festplattenspeicher für sich beansprucht.

Clustergrößen

NTFS verwendet – wie FAT32 – Cluster. Die Größe entspricht der Blockgröße, sofern es sich nicht um sehr große Partitionen handelt. Tabelle 9.3 zeigt die Standard-Clustergrößen für NTFS.

Laufwerkkapazität	Clustergröße
7 MB bis 16 TB	4 KB
16 bis 32 TB	8 KB
32 bi 64 TB	32 KB
64 bis 128 TB	64 KB
128 bis 256 TB	128 KB

Tabelle 9.3: NTFS-Clustergrößen

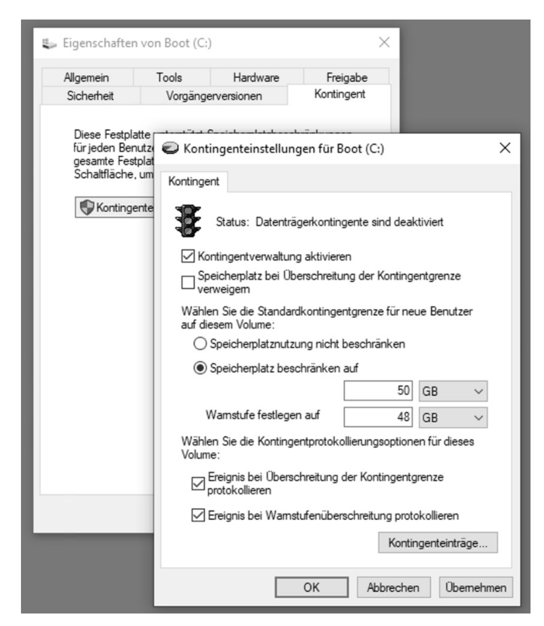


Abb. 9.25: Datenträgerkontingente in Windows 10

Standardmäßig unterstützt NTFS Partitionen mit bis zu etwa 16 Terabyte Kapazität bei dynamischen Datenträgern (2 Terabyte bei Basisfestplatten). Durch die Anpassung der Clustergrößen können Sie NTFS dazu bringen, Partitionen mit bis zu 16 Exabyte oder 18.446.744.073.709.551.616 Byte zu unterstützen! Damit dürfte Ihr Bedarf an Festplattenkapazitäten in den nächsten 100 Jahren wahrscheinlich abgedeckt sein.

Wichtig

NTFS unterstützt standardmäßig Partitionen mit bis zu 16 TB Kapazität.

Woher wissen Sie, welches der vielen Dateisysteme Sie verwenden sollen? Bei internen Festplatten sollten Sie das System mit den meisten Funktionen einsetzen, das Ihr Betriebssystem unterstützt. Wenn Sie eine aktuelle Windows-Version einsetzen, sollten Sie NTFS verwenden. FAT32 wird häufig für externe Festplatten und RAM-Sticks verwendet, weil NTFS-Funktionen wie die Zugriffssteuerungsliste und die Verschlüsselung den Zugriff erschweren können, wenn das Laufwerk oder der Stick an unterschiedlichen Systemen angeschlossen wird. Dies ist jedoch die einzige Ausnahme, und all die Vorteile von NTFS machen es zur besten Wahl für Windows-basierte Systeme.

9.2.4 exFAT

USB-RAM-Sticks erfreuen sich größter Beliebtheit. Ihre einfache und bequeme Verwendbarkeit machen Sie für Leute, die Freude daran haben, Programme, Fotos oder Wiedergabelisten mit anderen zu teilen, unentbehrlich. Heutzutage sind die Dateien dabei oft von erheblicher Größe, aber die RAM-Sticks sind ebenfalls mit stetig wachsender Kapazität erhältlich. Die zunehmende Speicherkapazität führt jedoch zu einem Problem mit dem Dateisystem.

Das seit Jahren auf RAM-Sticks übliche Dateisystem FAT32 funktioniert bei Laufwerken mit mehr als 2 TB nicht mehr. Von größerer Bedeutung ist jedoch, dass die Größe einer einzelnen Datei auf 4 GB beschränkt ist. Da es mittlerweile häufig erforderlich ist, Dateien zu transportieren, die erheblich größer als 4 GB sind, hat Microsoft sich Gedanken über einen Ersatz für FAT32 gemacht.

Wichtig

FAT32 unterstützt nur Laufwerke mit einer Größe von bis zu 2 TB und beschränkt die Größe einzelner Dateien auf 4 GB.

Das neue Dateisystem namens *exFAT* (*Extended File Allocation Table*) überspringt die Grenze von 4 GB und unterstützt Dateigrößen von 16 Exabyte (EB) sowie eine Partitionsgröße von theoretisch 64 Zettabyte (ZB). Microsoft empfiehlt eine Partitionsgröße von bis zu 512 TB für die heutigen größeren USB-Speichersticks, was fürs Erste genügen dürfte. Das exFAT-Dateisystem erweitert die 32-Bit-Clustereinträge der Dateiliste auf 64 Bit. Allerdings fehlen exFAT, ebenso wie FAT32, die erweiterten NTFS-Funktionen wie Zugriffsrechte, Komprimierung und Verschlüsselung.

Hinweis

1 Exabyte = 2^{60} Bytes und 1 Zettabyte = 2^{70} Bytes. Zum Vergleich: 1 Terabyte = 2^{40} Bytes. Wie Sie vom Rechnen mit Binärzahlen wissen, wird der Wert durch jede Erhöhung des Exponenten verdoppelt. Also sind 2^{41} Bytes = 2 TB, 2^{42} Bytes = 4 TB usw. Langer Rede, kurzer Sinn: Ein Zettabyte ist richtig, RICHTIG groß!

9.2.5 Dateisysteme in macOS

Apple ist derzeit dabei, das für Macs verwendete Dateisystem zu ändern. Das klassische Dateisystem für Macs ist *HFS+* (*Hierarchical File System Plus*). Für Time-Machine-Laufwerke wird es weiterhin benötigt, aber alle neuen Macs (und solche, auf denen macOS aktualisiert wird) verwenden APFS (*Apple File System*). Ebenso wie Windows und Linux kann macOS verschiedene Dateisysteme lesen und schreiben, wie etwa FAT32, und exFAT, NTFS kann es allerdings nur lesen.

9.2.6 Dateisysteme in Linux

Die meisten Linux-Distributionen verwenden ein Dateisystem, das unter der Bezeichnung *ext4* (*Fourth Extended File System*) bekannt ist. Ältere Distributionen verwenden eine der Vorgängerversionen, wie etwa ext3 oder ext2. Das ext4-Dateisystem unterstützt Volumes mit einer Größe von bis zu 1 Exabyte (EB) und Dateigrößen von bis zu 16 TB und ist zu ext3 und ext2 abwärtskompatibel. Sie können also beispielsweise ein ext3-Laufwerk problemlos als ext4-Volume mounten. Sie müssen keine Einzelheiten über ext4 oder ext3 wissen, lediglich, dass es sich um Linux-Dateisysteme handelt und dass ext4 Volumegrößen von bis zu 1 EB und Dateigrößen von bis zu 16 TB unterstützt.

Hinweis

Linux-Dateisysteme sind flexibler als die in macOS und Windows verfügbaren. Sie können auf NTFS, FAT32, exFAT, HFS+ sowie auf ext4, ext3 und ext2 lesend und schreibend zugreifen. Nett!

Viele Linux-Distributionen, insbesondere die in großen Datenzentren eingesetzten, verwenden das Dateisystem ZFS oder dessen neueren Verwandten BTRFS (sprich: »Butter Eff Ess«). Beide bieten beim Kopieren und der Datenträgerverwaltung leistungsfähige Merkmale, die weit über den Rahmen der CompTIA A+-Prüfung hinausgehen. Für weitere Informationen zu ZFS, das wohl die Zukunft darstellt (auch in Windows), ist der Wikipedia-Artikel ein guter Ausgangspunkt. Folgen Sie den Links zu den Quellen.

9.3 Partitionierung, Formatierung und Speicherpools

Nachdem Sie die Grundlagen zur Formatierung und Partitionierung kennengelernt haben, möchte ich Ihnen zeigen, wie eine eingebaute Festplatte unter Verwendung unterschiedlicher Werkzeuge für die Partitionierung und Formatierung eingerichtet wird. Am Ende dieses Abschnitts werden wir durch das Anlegen virtueller Festplatten einen Speicherpool erstellen. Wenn Sie Zugriff auf ein System haben, probieren Sie die hier beschriebenen Dinge aus. Nehmen Sie aber keinesfalls Änderungen an einem Laufwerk vor, mit dem Sie noch arbeiten wollen, weil die Partitionierung, die Formatierung und die Einrichtung von Speicherpools zerstörerische Vorgänge sind! Ohne einige Laufwerke, deren Inhalte entbehrlich sind, werden Sie die Vorgänge nicht nachvollziehen können.

9.3.1 Startfähige Datenträger

Angenommen, Sie richten einen ganz neuen PC ein. Auf der Festplatte befindet sich kein Betriebssystem, deshalb müssen Sie irgendetwas booten, um diese Festplatte einrichten zu können. Bootfähige Software ist per definitionem ein Betriebssystem. Sie brauchen also einen optischen Datenträger oder einen USB-Stick, auf denen ein startfähiges Betriebssystem installiert ist. Wechseldatenträger, die ein startfähiges Betriebssystem enthalten, werden im Allgemeinen als System- oder Startdatenträger bezeichnet. Ihr System bootet vom Startdatenträger, der dann eine Art Betriebssystem lädt, mit dem Sie Ihre neue Festplatte partitionieren, formatieren und ein Betriebssystem darauf installieren können. Startdatenträger können unterschiedlichster Herkunft sein. Alle Installations-Discs von Windows (Abbildung 9.26) und Linux sind startfähig.



Abb. 9.26: Startfähige Datenträger

Mache Startdatenträger enthalten eine *Image-Datei* (Festplattenabbild) eines Installationsmediums, das für gewöhnlich in Form einer Datei mit der Endung `.iso` gespeichert ist. Image-Dateien werden oft auf herkömmlichen Installationsmedien wie CD, DVD oder USB-Stick gespeichert, können im Prinzip jedoch an beliebiger Stelle abgelegt werden, z.B. auf einem Netzlaufwerk.

Alle startfähigen Datenträger bringen irgendein Werkzeug zum Partitionieren von Laufwerken und zum Formatieren einer neuen Partition mit. Um auf einem Laufwerk ein Betriebssystem zu installieren, sind eine Partitionierung und eine Formatierung unverzichtbar.

9.3.2 Partitionieren und Formatieren mit den Installationsmedien

Wenn Sie von einem Windows-Installationsmedium booten und das Installationsprogramm eine noch nicht partitionierte Festplatte erkennt, führt es Sie durch die Schritte zur Partitionierung und Formatierung der Festplatte. In Kapitel 11, *Der maßgeschneiderte PC*, wird der gesamte Installationsprozess beschrieben. Hier greife ich daher ein wenig vor und beginne direkt mit der Partitionierung.

Partitionierung und Formatierung sind mit aktuellen Windows-Versionen ziemlich unkompliziert. Während des Installationsvorgangs durchlaufen Sie eine Reihe von Bildschirmen (Abbildung 9.27), auf denen Sie die Sprache auswählen, nach dem *Product Key* gefragt und um Zustimmung zur Lizenzvereinbarung gebeten werden. Schließlich gelangen Sie zum Dialogfeld WO MÖCHTEN SIE WINDOWS INSTALLIEREN? (Abbildung 9.28).

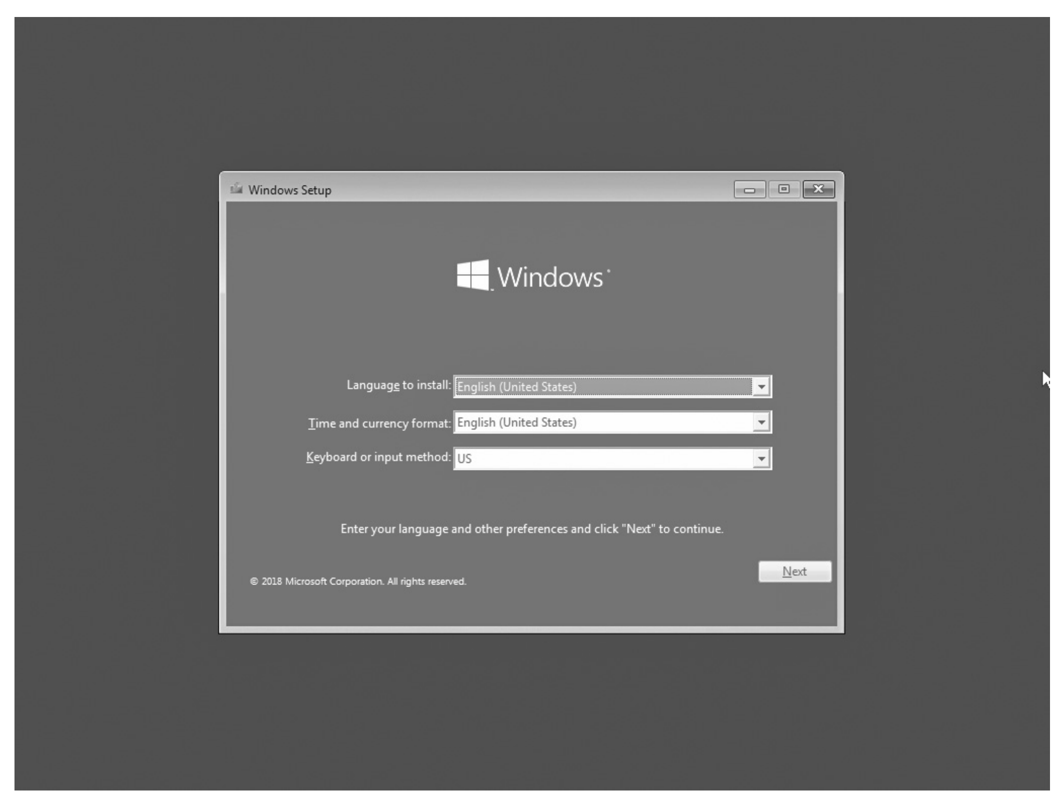


Abb. 9.27: Sprach-, Währungs- und Tastatureinstellungen bei der Installation

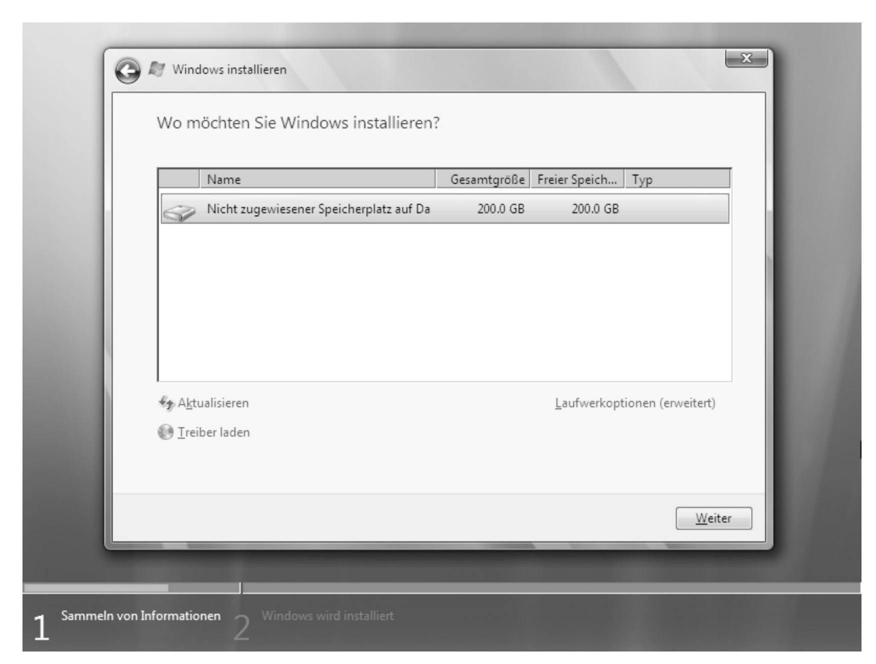


Abb. 9.28: Wo möchten Sie Windows installieren?

Die häufigste Installationsvariante ist diejenige mit einer einzigen aktiven Partition `C:`, die als NTFS formatiert wird. Beachten Sie, dass Windows zwei Partitionen anlegt, eine für das System reservierte Partition und die `C:`-Partition. Das ist völlig normal und vom System so beabsichtigt. Abbildung 9.29 zeigt eine typische Windows-Installation in der Datenträgerverwaltung.

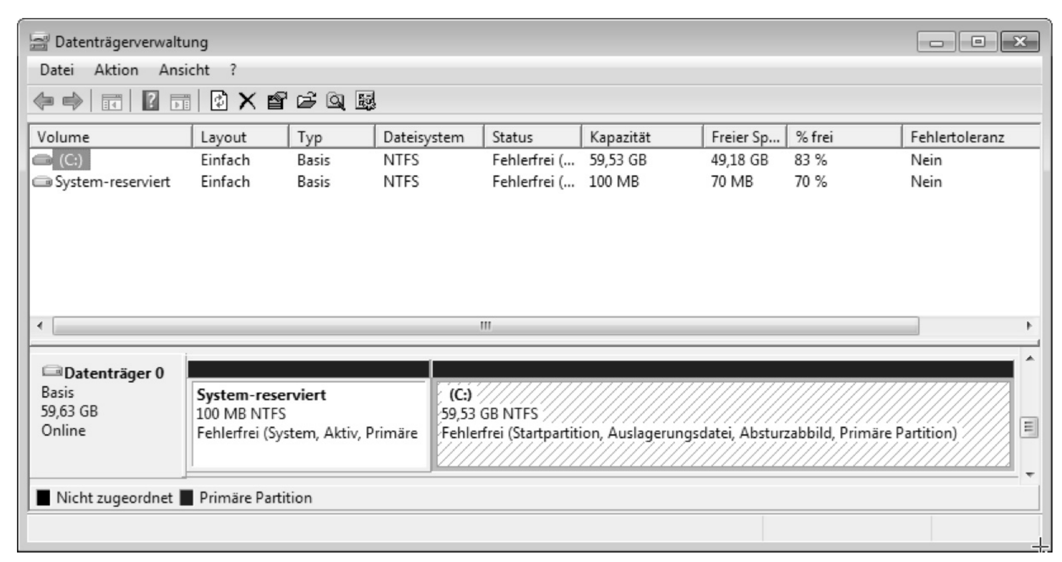


Abb. 9.29: Typische Windows-Installation in der DATENTRÄGERVERWALTUNG

Klicken Sie im Dialogfeld WO MÖCHTEN SIE WINDOWS INSTALLIEREN? die Schaltfläche LAUFWERK-OPTIONEN (ERWEITERT) an, wenn Sie eine eigene Partition anlegen oder vorhandene löschen möchten. Um eine neue Partition zu erstellen, klicken Sie die Schaltfläche NEU an. Geben Sie für die neue Partition eine Größe in Gigabyte ein und klicken Sie danach auf ÜBERNEHMEN. In Windows 10 erscheint ein Hinweis, dass Windows möglicherweise eine weitere Partition für Systemdateien anlegt. Wenn Sie nun auf OK klicken, werden die für das System reservierte Partition sowie die von Ihnen festgelegte Partition angelegt (Abbildung 9.30). Der übrige Plattenplatz wird als NICHT ZUGEWIESENER SPEICHERPLATZ angezeigt.

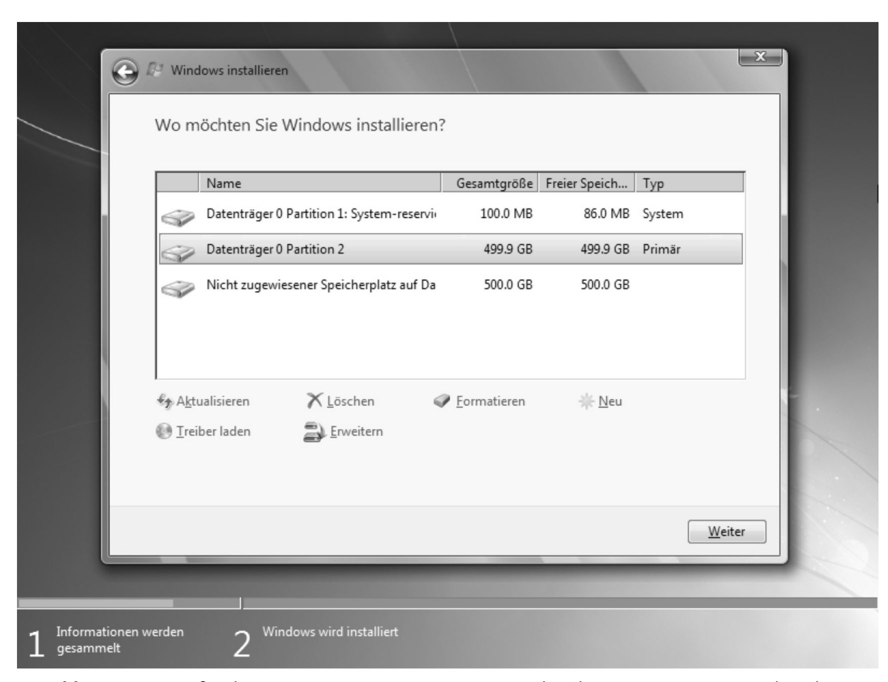


Abb. 9.30: Neue für das System reservierte Partition und nicht zugewiesener Speicherplatz

Klicken Sie nach dem Erstellen der Partition auf FORMATIEREN. Das Installationsprogramm fragt Sie hier nicht danach, welches Dateisystem verwendet werden soll, sondern verwendet NTFS. Neuere Windows-Versionen können zwar mit FAT32-Laufwerken umgehen, Sie können diese Betriebssysteme jedoch standardmäßig nicht darauf installieren.

Im Beispiel sehen Sie eine 1-TB-Festplatte mit einer 499-GB-Partition und 500 GB nicht zugewiesenem Speicherplatz. Wenn Sie es sich später anders überlegen und die Partition das gesamte Terabyte verwenden soll, was wäre dann zu tun? Klicken Sie einfach auf ERWEITERN und weisen Sie der Partition, die Sie gerade formatiert haben, den verbleibenden Speicherplatz zu. Diese Funktion ermöglicht es Ihnen, unpartitionierte Bereiche einem bereits partitionierten Laufwerk mit einem Mausklick hinzuzufügen.

9.3.3 Datenträgerverwaltung

Das eigentliche Werkzeug für die Partitionierung und Formatierung ist die Datenträgerverwaltung. Abbildung 9.31 zeigt das Werkzeug unter Windows 7. Microsoft hat die Benutzeroberfläche in den nachfolgenden Windows-Versionen nicht geändert. Über die Datenträgerverwaltung können Sie so ziemlich alle im Zusammenhang mit der Vorbereitung von Festplatten oder SSDs anfallende Arbeiten mit einem praktischen Werkzeug erledigen, unter anderem Initialisierung, Volumes erstellen, dynami-

sche Laufwerke erstellen, Laufwerke erweitern und anderes mehr. Klicken Sie mit der rechten Maustaste auf das Startmenü oder geben Sie »Datenträgerverwaltung« in das Suchfeld ein, um das Werkzeug zu starten.

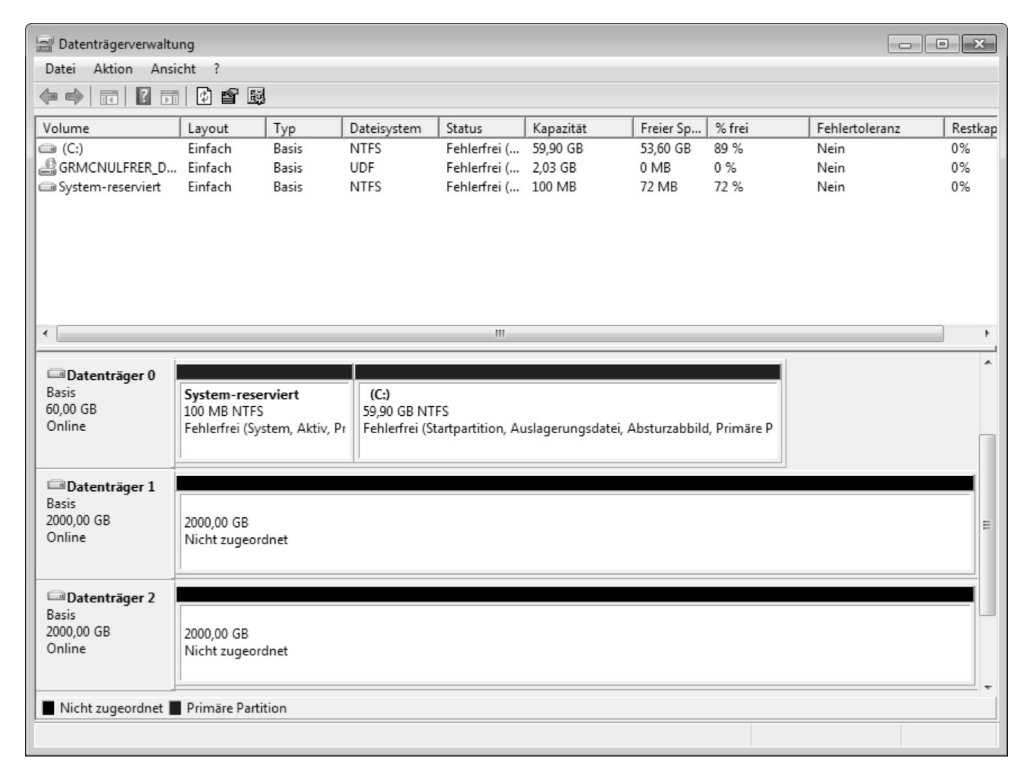


Abb. 9.31: Die Datenträgerverwaltung

Hinweis

Windows bietet ein Kommandozeilenwerkzeug zur Verwaltung von Massenspeichergeräten namens `diskpart`, der Nachfolger von `FDISK`. Es ist außerordentlich leistungsfähig (und gefährlich, wenn man es ohne die nötigen Kenntnisse verwendet). Kapitel 16 geht ausführlicher auf `diskpart` ein.

Festplatteninitialisierung

Auf jeder Festplatte in einem Windows-System werden spezielle Daten geschrieben. Diese Initialisierungsdaten umfassen Kennungen, die das Laufwerk einem System zuordnen, und weitere Daten zur Beschreibung der Funktion der Festplatte im System. Wenn die Festplatte beispielsweise zu einem RAID-Verbund gehört, werden die RAID-Informationen bei der Initialisierung gespeichert. Wenn sie Teil eines übergreifenden Datenträgers ist, wird das ebenfalls dort festgehalten.

Alle neuen Laufwerke müssen initialisiert werden, bevor sie benutzt werden können. Wenn Sie eine zusätzliche Festplatte in einem Windows-System installieren und die Datenträgerverwaltung starten, erkennt das System die neue Festplatte und startet den Assistenten für die Initialisierung der Festplatte. Falls Sie den Assistenten nicht ausführen, wird das Laufwerk als unbekannt aufgelistet (Abbildung 9.32).

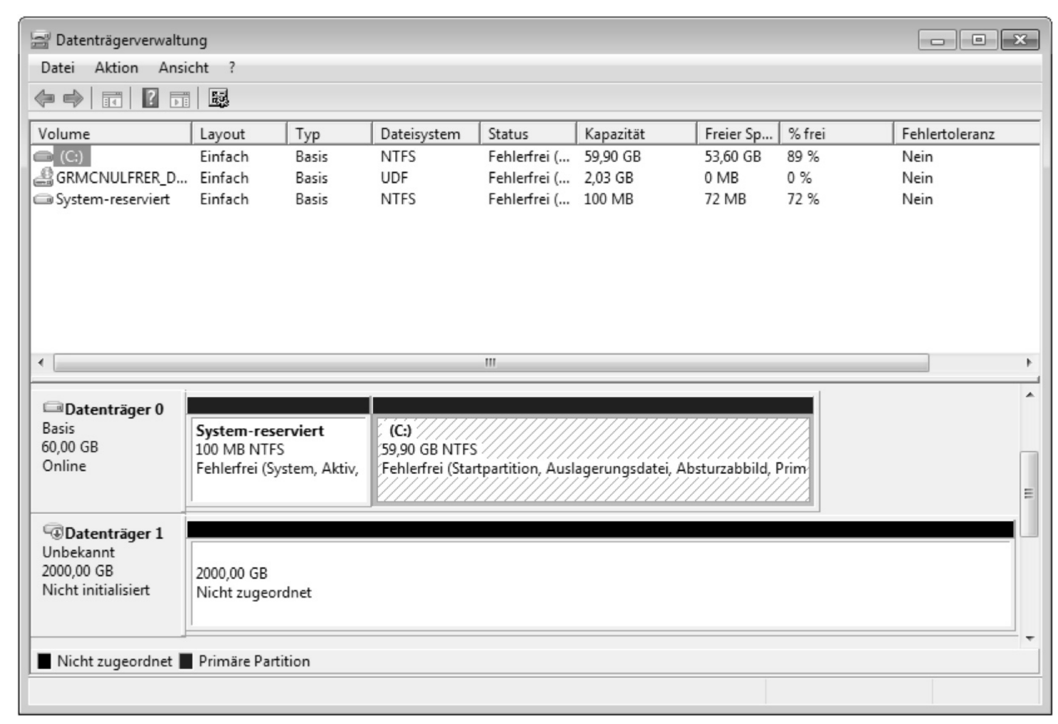


Abb. 9.32: Unbekanntes Laufwerk in der Datenträgerverwaltung

Um eine Festplatte zu initialisieren, klicken Sie das Festplattensymbol mit der rechten Maustaste an und wählen im Kontextmenü INITIALISIEREN. Sie haben dann die Möglichkeit, als Partitionsschema MBR oder GPT auszuwählen (Abbildung 9.33). Nach der Initialisierung der Festplatte wird deren Status angezeigt, was bei der Fehlersuche recht praktisch sein kann.

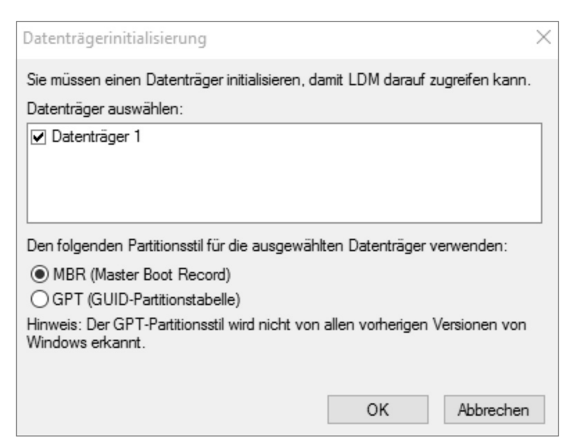


Abb. 9.33: Datenträgerinitialisierung

In der Datenträgerverwaltung wird der Status aller Datenträger des Systems aufgeführt. Hoffentlich sehen Sie bei allen aufgeführten Laufwerken den Hinweis »Fehlerfrei«, der anzeigt, dass sie in Ordnung sind und reibungslos funktionieren. Die beiden Zustände »Nicht zugeordnet« und »Aktiv« ken-

nen Sie ebenfalls bereits. Für die CompTIA A+-Prüfungen und als praktisch tätiger Techniker sollten Sie aber auch die folgenden noch kennen:

- **Unbekannt**: Dieser Status wird z.B. angezeigt, wenn Sie einen dynamischen Datenträger in einen anderen Computer einbauen.
- **Formatiere**: Wie Sie sich denken können, wird dieser Status beim Formatieren eines Datenträgers angezeigt.
- **Fehler**: Diesen Status bekommen Sie hoffentlich nie zu sehen, denn er bedeutet, dass die Festplatte beschädigt ist oder fehlerhafte Daten enthält. Wahrscheinlich ist es zu Datenverlusten gekommen.
- **Online**: Wird angezeigt, wenn eine Festplatte fehlerfrei funktioniert und mit dem Rechner kommuniziert.
- **Offline**: Die Festplatte ist entweder defekt oder hat Probleme, mit dem Rechner zu kommunizieren.

Ein neu installiertes Laufwerk wird immer als Basisfestplatte eingerichtet. Es gibt nichts daran auszusetzen, Basisfestplatten zu verwenden, aber Sie werden dann auf einige praktische Funktionen verzichten müssen.

Partitionen und Volumes erstellen

Um Partitionen zu erstellen, klicken Sie mit der rechten Maustaste den nicht zugeordneten Teil des Laufwerks an und wählen im Kontextmenü NEUES EINFACHES VOLUME aus. Die Datenträgerverwaltung führt den Assistenten zum Erstellen neuer einfacher Volumes aus. Nun wird ein Dialogfeld angezeigt, in dem Sie die gewünschte Größe des Volumes angeben können. (Abbildung 9.34).

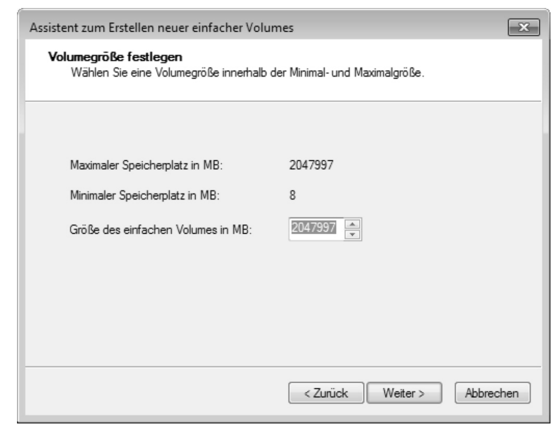


Abb. 9.34: Angabe der Volumegröße

Legen Sie eine Partitionsgröße fest und klicken Sie auf WEITER. Nun fragt Sie der Assistent, ob Sie dem Volume einen Laufwerksbuchstaben zuweisen möchten, es als Ordner auf einem vorhandenen Volume bereitstellen wollen oder nichts von beidem (Abbildung 9.35). In fast allen Fällen werden Sie einer Primärpartition oder einem einfachen Volume einen Laufwerksbuchstaben zuweisen wollen.

Hinweis

Es ist hier wichtig, darauf hinzuweisen, dass es unter den aktuellen Windows-Versionen beim Erstellen eines Volumes auf einem MBR-Laufwerk keine Auswahlmöglichkeit zwischen primärer oder erweiterter Partition gibt. Die ersten drei Volumes, die Sie anlegen, gehören zur primären Partition. Alle weiteren sind dann logische Laufwerke auf einer erweiterten Partition. Das Kommandozeilenwerkzeug `diskpart` bietet Optionen, die in der Datenträgerverwaltung nicht verfügbar sind. Details finden Sie in Kapitel 16.

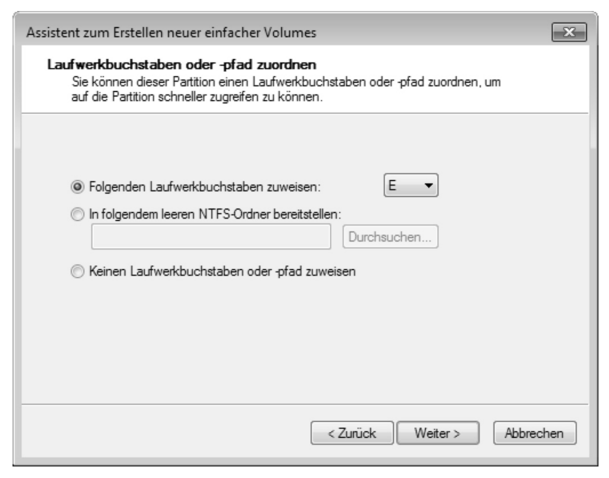


Abb. 9.35: Einen Laufwerksbuchstaben zuweisen

Das letzte Dialogfeld beim Erstellen des neuen einfachen Volumes fragt Sie nach dem Format, das dafür verwendet werden soll (Abbildung 9.36). Wenn Ihre Partition 32 GB groß oder kleiner ist, können Sie diese als FAT32 oder NTFS formatieren. Bei Partitionen, die größer als 32 GB sind, unterstützt die Datenträgerverwaltung nur noch NTFS. Zwar unterstützt FAT32 auch Partitionen bis zu 2 TB, Microsoft fordert aber die Verwendung von NTFS für größere Partitionen und hat daher diese künstliche Obergrenze eingeführt. Angesichts der heutigen Festplattenkapazitäten gibt es aber auch keinen Grund, NTFS nicht zu verwenden. Neben der Auswahl eines Dateisystems gibt es in diesem Dialogfeld das Kontrollkästchen SCHNELLFORMATIERUNG DURCHFÜHREN. Wie Sie bereits wissen, wird bei der Schnellformatierung keine Überprüfung der Cluster der Festplatte vorgenommen, während diese bei der vollständigen Formatierung stattfindet.

Wichtig

Den Unterschied zwischen einer Schnellformatierung und einer vollständigen Formatierung sollten Sie kennen.

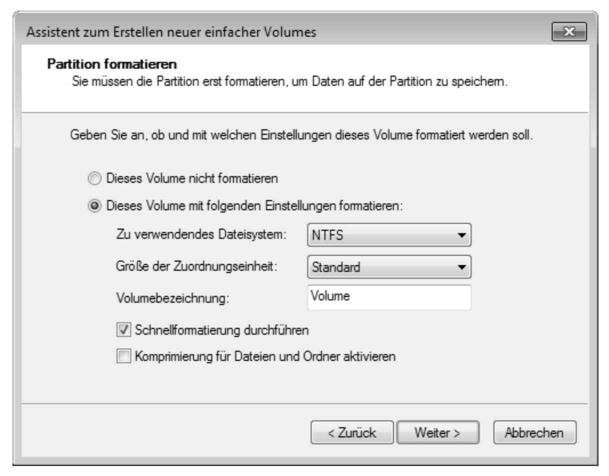


Abb. 9.36: Auswahl eines Dateisystems

In diesem Dialogfeld müssen Sie mehrere Aufgaben erledigen. Sie können eine Datenträgerbezeichnung festlegen. Außerdem können Sie die Clustergröße (Größe der Zuordnungseinheiten) festlegen, wofür es allerdings normalerweise keinen Grund gibt, behalten Sie die Standardwerte also besser bei. Sie können aber natürlich das Formatieren beschleunigen, wenn Sie das Kontrollkästchen SCHNELLFORMATIERUNG DURCHFÜHREN aktivieren. Damit wird Ihr Laufwerk formatiert, ohne dass die Cluster einzeln überprüft werden. Das ist schnell und etwas riskant, aber neue Festplatten kommen so gut wie immer fehlerfrei aus dem Werk – Sie müssen also selbst entscheiden, ob Sie das tun wollen oder nicht.

Wenn Sie schließlich NTFS auswählen, können Sie die Datei- und Ordnerkomprimierung aktivieren. Wenn Sie diese Option verwenden, können Sie jede Datei und jeden Ordner innerhalb der Partition mit der rechten Maustaste anklicken und sie komprimieren. Wählen Sie dazu im Kontextmenü EIGENSCHAFTEN und klicken Sie anschließend die Schaltfläche ERWEITERT an, um zu den entsprechenden Optionen zu gelangen (Abbildung 9.37). Die Komprimierung ist praktisch, um ein wenig Platz auf einer vollen Festplatte zu schaffen.

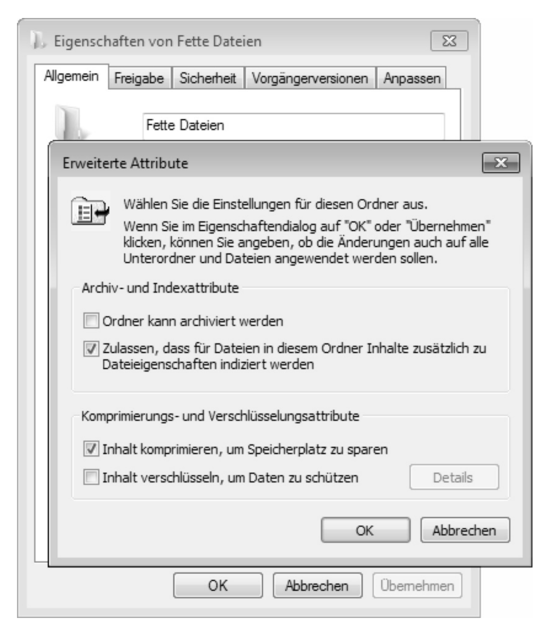


Abb. 9.37: Aktivieren der Komprimierung

Dynamische Datenträger

Dynamische Datenträger werden in der Datenträgerverwaltung aus Basisfestplatten erstellt. Nachdem Sie ein Laufwerk von einer Basisfestplatte in einen dynamischen Datenträger umgewandelt haben, gibt es keine primären und erweiterten Partitionen mehr. Dynamische Datenträger werden in Volumes statt in Partitionen unterteilt. Da in aktuellen Windows-Versionen Partitionen als Volumes bezeichnet werden, wird die Konvertierung zu einem dynamischen Datenträger überhaupt nicht mehr deutlich.

Wichtig

Wenn Sie einen dynamischen Datenträger aus einem Rechner in einen anderen einbauen, dann wird er in der Datenträgerverwaltung als unbekanntes Laufwerk angezeigt. Sie können Fremdlaufwerke aber in ein neues System importieren, wenn Sie deren Symbol anklicken und im Kontextmenü die entsprechende Option anklicken.

Um eine Basisfestplatte in einen dynamischen Datenträger umzuwandeln, klicken Sie einfach das Festplattensymbol mit der rechten Maustaste an und wählen In dynamischen Datenträger konvertieren (Abbildung 9.38). Das geht schnell und gefahrlos, aber nicht in der umgekehrten Richtung. Um einen dynamischen Datenträger in eine Basisfestplatte umzuwandeln, müssen sie zuerst alle Volumes von der Festplatte löschen.

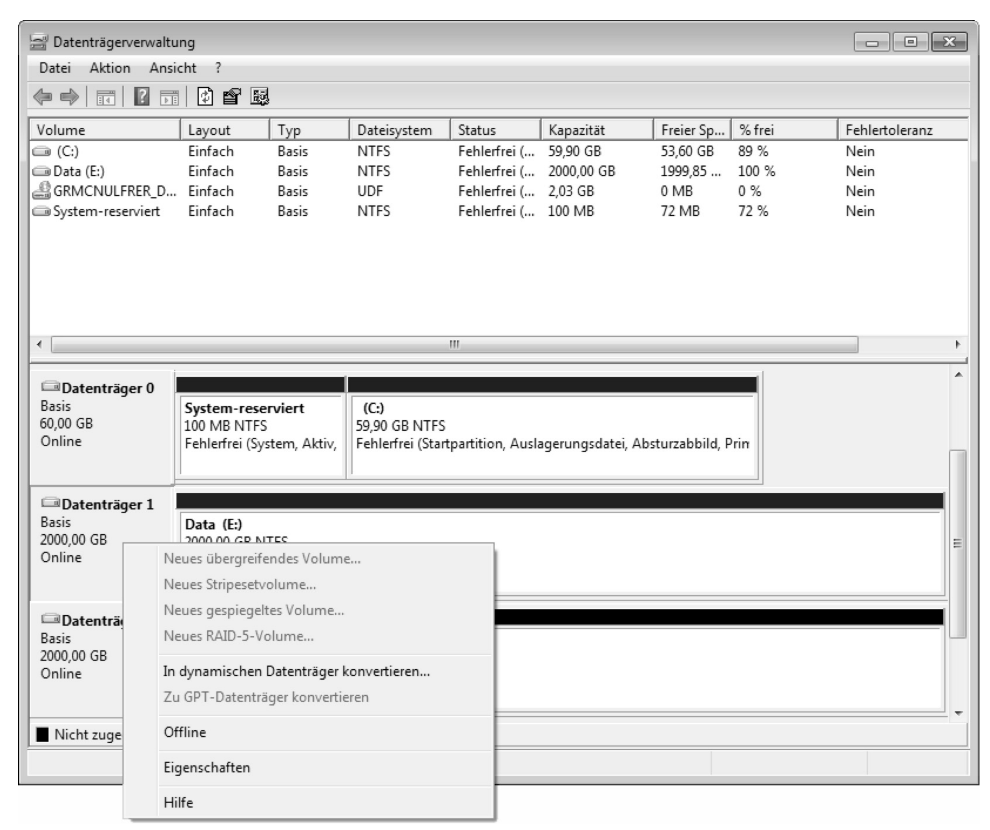


Abb. 9.38: Umwandlung in einen dynamischen Datenträger

Nach Abschluss der Umwandlung können Sie fünf Arten von Volumes auf dynamischen Datenträgern anlegen: einfach, übergreifend, Stripeset, gespiegelt und RAID 5. Als Nächstes lernen Sie, wie die drei gebräuchlichsten Datenträgertypen implementiert werden. Im letzten Schritt weisen Sie einen Laufwerksbuchstaben zu oder stellen den Datenträger als Ordner bereit.

Einfache Volumes Ein einfaches Volume verhält sich genau wie eine primäre Partition. Wenn es in einem System nur einen dynamischen Datenträger gibt, kann es nur ein einfaches Volume besitzen. Beachten Sie hier unbedingt, dass sich ein einfaches Volume zwar genau wie eine traditionelle primäre Partition verhält, aber doch etwas völlig anderes ist, denn Sie können darauf kein Betriebssystem installieren.

Klicken Sie in der Datenträgerverwaltung nicht zugeordneten Speicherplatz auf dem dynamischen Datenträger mit der rechten Maustaste an und wählen Sie Neues einfaches Volume (Abbildung 9.39), um den Assistenten zum Erstellen eines neuen einfachen Volumes auszuführen. Es werden Ihnen dann noch mehrere Dialogfelder angezeigt, in denen Sie nach Größe und Art des zu verwendenden Dateisystems gefragt werden. Abbildung 9.40 zeigt die Datenträgerverwaltung mit drei neu angelegten einfachen Volumes.

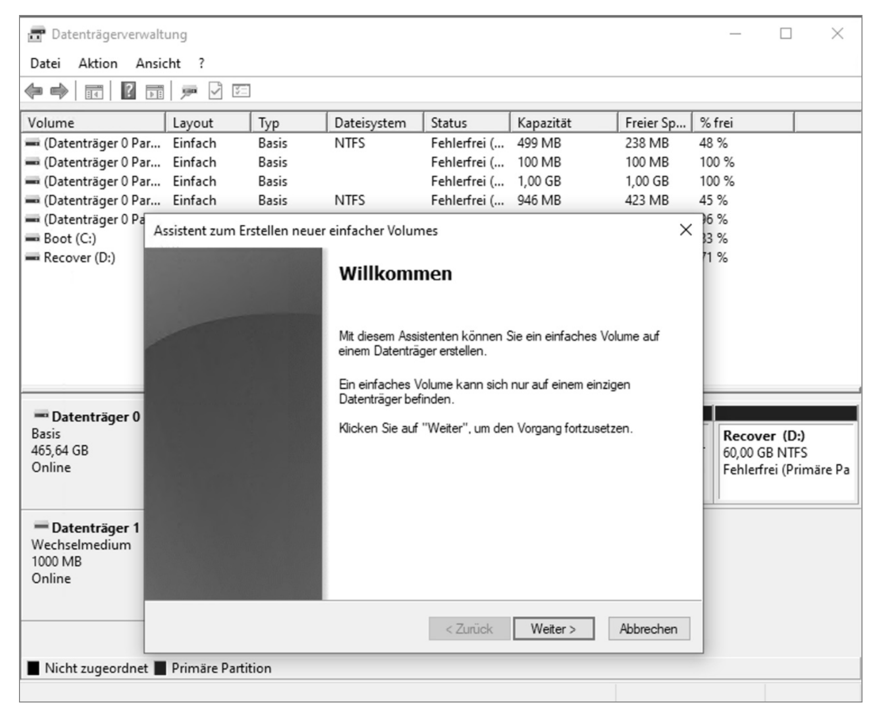


Abb. 9.39: Assistent zum Erstellen neuer Volumes aufrufen

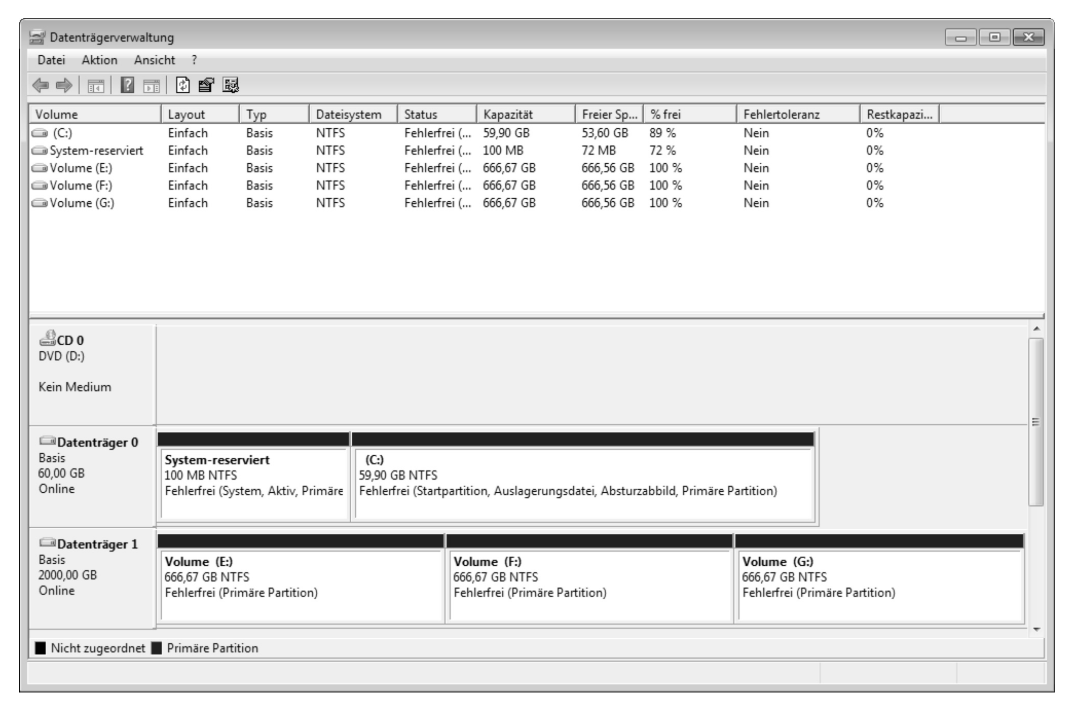


Abb. 9.40: Drei einfache Volumes auf einem dynamischen Datenträger

Übergreifende Volumes Bei dynamischen Datenträgern können Sie die Größe eines einfachen Volumes auf den gesamten nicht zugeordneten Speicherplatz eines dynamischen Datenträgers erweitern. Sie können den Datenträger auch über einen anderen dynamischen Datenträger (und damit eine andere Festplatte) erweitern und so übergreifende Volumes erstellen. Um das zu vergrößernde Volume zu erweitern oder übergreifend zu machen, klicken Sie es einfach mit der rechten Maustaste an und wählen im Kontextmenü VOLUME ERWEITERN an (Abbildung 9.41). Der Assistent zum Erweitern von Volumes wird angezeigt und fragt Sie nach der Position des freien Speicherplatzes auf einem dynamischen Datenträger und nach der Gesamtgröße des erweiterten Volumes (Abbildung 9.42). Bei mehreren vorhandenen Laufwerken können Sie das Volume auch auf eines der anderen Laufwerke ausweiten.

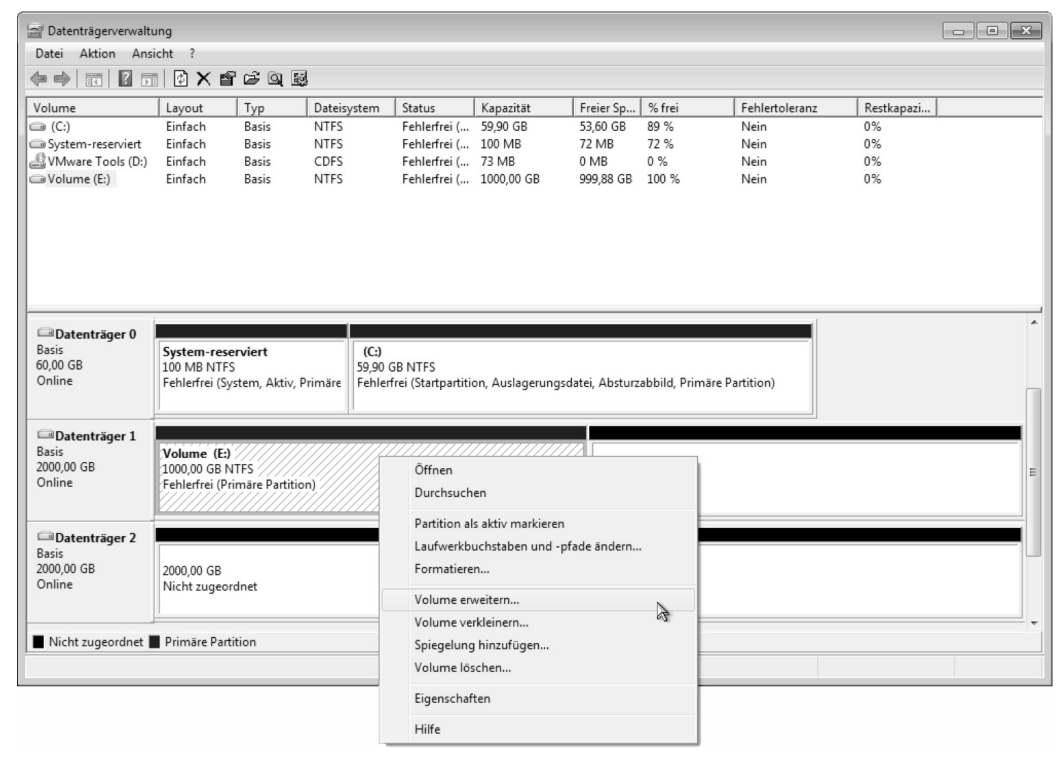


Abb. 9.41: Auswahl der Option VOLUME ERWEITERN

Dynamische Datenträger sind Gold wert, weil sich mit ihnen Volumes erweitern und übergreifend definieren lassen. Wenn Sie auf einem Volume keinen Platz mehr haben, bauen Sie einfach eine neue physische Festplatte in das System ein und erweitern das Volume auf das neue Laufwerk. Auf diese Weise bleiben die Laufwerksbuchstaben konsistent und unverändert, sodass Ihre Programme nicht durcheinander kommen, und trotzdem können Sie die Festplattenkapazitäten bei Bedarf jederzeit erweitern.

Vorsicht

Nach der Umwandlung in einen dynamischen Datenträger gehen alle Daten verloren, wenn Sie ihn wieder in eine Basisfestplatte konvertieren wollen. Vor solch einer Umwandlung müssen Sie unbedingt alle Daten sichern!



Abb. 9.42: Der Assistent zum Erweitern von Volumes

Sie können jedes einfache Volume auf einem dynamischen Datenträger erweitern oder übergreifend machen, nicht nur dasjenige »am Ende« in der Datenträgerverwaltung. Sie wählen einfach das zu erweiternde Volume aus und geben an, wie weit es vergrößert werden soll. Abbildung 9.43 zeigt ein einfaches 477,54 GB großes Volume namens ERWEITERT, das um zusätzliche 1.332,03 GB von der Festplatte erweitert wurde, wobei der sich anschließende 190,43 GB große Abschnitt übersprungen wurde. Damit ist ein 1.809,57 GB großes Volume entstanden. Windows hat kein Problem damit, Bereiche auf einem Datenträger zu überspringen.

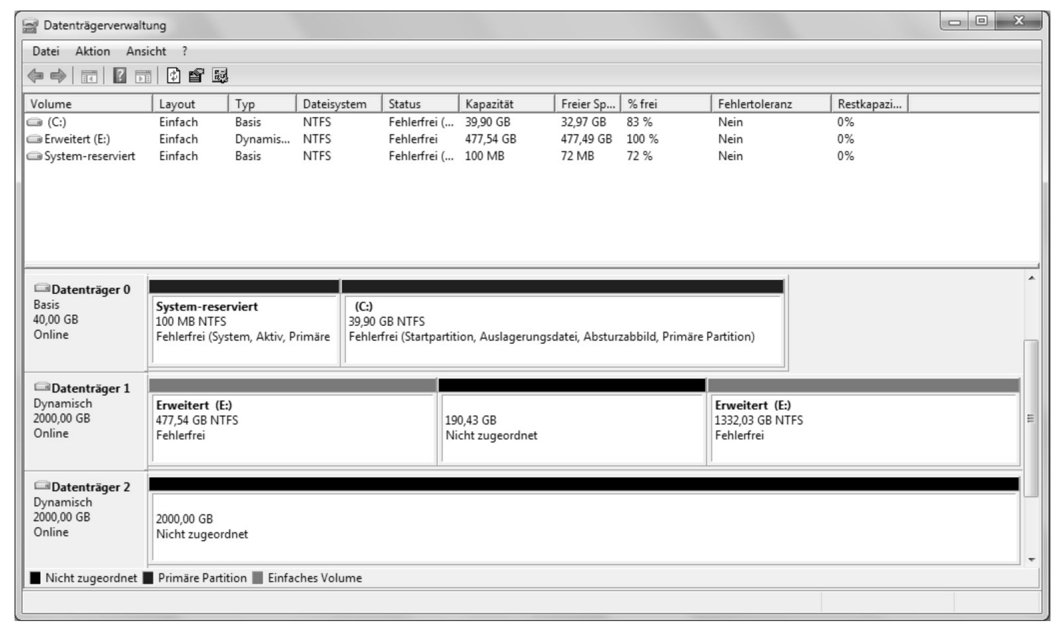


Abb. 9.43: Erweitertes Volume

Hinweis

Unter den aktuellen Windows-Versionen lassen sich Partitionen auch ohne die Verwendung von dynamischen Datenträgern vergrößern und verkleinern. Primärpartitionen mit freiem Speicher lassen sich verkleinern (allerdings wegen der Position möglicherweise vorhandener nicht verschiebbarer Bereiche wie dem MBR nicht immer um die gesamte freie Kapazität) und Sie können Partitionen auch vergrößern, wenn sich dahinter noch nicht partitionierte Bereiche anschließen.

Klicken Sie zum Verkleinern mit der rechten Maustaste auf eine Partition und wählen Sie VOLUME VERKLEINERN. Die Datenträgerverwaltung errechnet dann, um wie viel Speicherplatz Sie die Partition verkleinern können. Dann können Sie einen Betrag bis zu dieser Menge auswählen. Wählen Sie zum Vergrößern einer Partition nach dem Rechtsklick VOLUME ERWEITERN aus.

Stripesetvolumes Wenn in einem PC zwei oder mehr dynamische Datenträger verwendet werden, können Sie diese über die Datenträgerverwaltung zu einem *Stripesetvolume* kombinieren. Der Begriff »RAID 0« wird in der Datenträgerverwaltung zwar nicht verwendet, aber Sie wissen bereits, dass es sich um ein solches handelt. Ein Stripesetvolume verteilt die Blöcke einer Datei über mehrere Festplatten. Bei Verwendung von zwei oder mehr Laufwerken in einer als Stripeset bezeichneten Gruppe werden die Daten zuerst in eine bestimmte Anzahl an Clustern auf einem Laufwerk, dann auf dem nächsten Laufwerk usw. geschrieben. Damit erhöht sich der Datendurchsatz, weil das System nicht mehr so lange warten muss, um von einem Laufwerk zu lesen oder darauf schreiben zu können. Der Nachteil beim Striping ist, dass alle Daten in einem Stripeset verloren gehen, wenn eines der Laufwerke im Stripeset ausfällt.

Um ein Stripesetvolume zu erstellen, klicken Sie den freien Speicherplatz auf dem Laufwerk mit der rechten Maustaste an, wählen NEUES VOLUME und dann STRIPESET. Der Assistent fragt Sie nach dem anderen Laufwerk, das Sie dem Stripeset hinzufügen wollen. Sie müssen einen nicht zugeordneten Speicherbereich auf einem anderen dynamischen Datenträger auswählen. Wählen Sie diesen aus und durchlaufen Sie die weiteren Dialogfelder zur Größe und Formatierung, bis ein neuer Stripeset-Datenträger angelegt ist (Abbildung 9.44). Die beiden Stripes in der Abbildung sind zwar scheinbar unterschiedlich groß, aber bei genauerem Hinsehen lässt sich erkennen, dass sie beide 1.000 GB groß sind. Alle Stripes auf den verschiedenen Laufwerken müssen gleich groß sein.

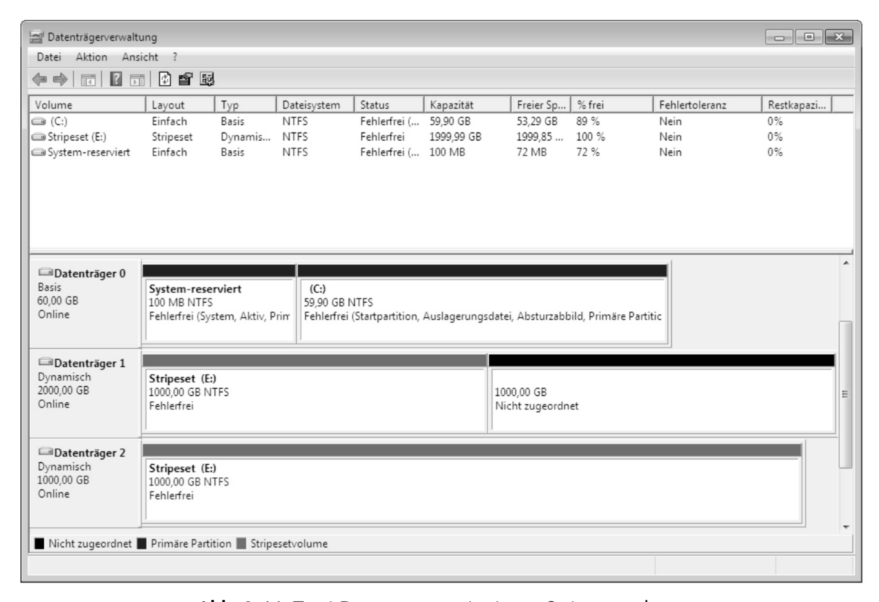


Abb. 9.44: Zwei Datenträger mit einem Stripesetvolume

Gespiegelte Volumes Windows 7 Professional, Enterprise und Ultimate sowie neuere Windows-Versionen können zwei Laufwerke zwecks Redundanz zu einer gespiegelten Festplatte zusammenschließen. Sie kennen das bereits aus Kapitel 8 unter dem Begriff RAID 1. Rechtsklicken Sie zum Einrichten auf freien Speicherplatz eines Laufwerks und wählen Sie NEUES GESPIEGELTES VOLUME (Abbildung 9.45). Nun startet der Assistent zum Erstellen eines gespiegelten Volumes. Klicken Sie auf WEITER, wählen Sie eines der verfügbaren Laufwerke aus und klicken Sie dann auf HINZUFÜGEN, um es der Liste der ausgewählten Laufwerke hinzuzufügen (Abbildung 9.46). Ein weiterer Klick auf WEITER führt zum bereits bekannten Dialogfeld, in dem ein Laufwerksbuchstabe oder -pfad zugewiesen wird.

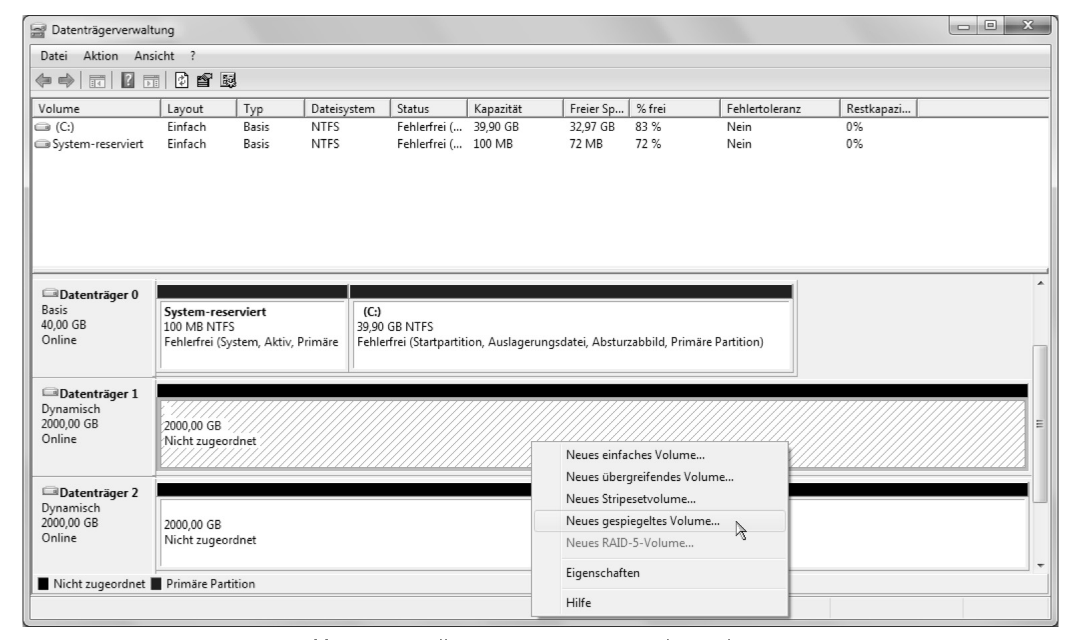


Abb. 9.45: Erstellen eines neuen gespiegelten Volumes



Abb. 9.46: Auswahl der Datenträger

Weitere RAID-Level Mit der Datenträgerverwaltung können Sie in allen Professional-Versionen von Windows als robuste Speicherlösung RAID-5-Arrays mit drei oder mehr Laufwerken einrichten. Zum Leidwesen der Benutzer dieser Betriebssysteme ist dies jedoch nur auf einem Windows-Server möglich, auf den Sie über ein Netzwerk zugreifen. (Seit den Professional- und Enterprise-Versionen von Windows 8 gibt es die sogenannten *Speicherplätze*, eine Möglichkeit, in Form von Speicherpools ein Pseudo-RAID zu realisieren. Eine der Optionen hat große Ähnlichkeit mit RAID 5. Mehr dazu im Abschnitt 9.3.5, *Speicherplätze*.)

Verschachtelte RAID-Arrays werden von der Datenträgerverwaltung nicht unterstützt. Falls Sie ein RAID 0+1 oder ein RAID 1+0 (RAID 10) verwenden möchten, müssen Sie ein Hardware-RAID einsetzen.

Bereitstellen von Laufwerken als Ordner

Partitionen und Volumes kann nicht nur ein Laufwerksbuchstabe von `D:` bis `Z:` zugewiesen werden, sie lassen sich auf anderen Laufwerken auch als Ordner in Form eines *Bereitstellungspunkts* bereitstellen. Auf diese Weise können Sie in bereits vorhandenen Ordnern mehr Daten ablegen, als auf ein einzelnes Laufwerk oder ein einzelnes Volume passen würde (Abbildung 9.47).

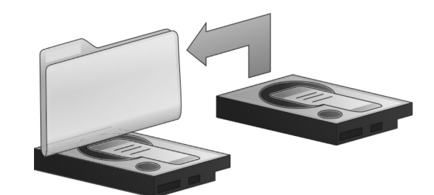


Abb. 9.47: Ein als Ordner bereitgestelltes Volume

Nehmen wir an, Sie verwenden auf Ihrem Rechner mit Windows den Ordner DOKUMENTE, um Ihre digitalen Fotos zu speichern. Bald stellen Sie fest, dass Ihre Sammlung schnell wächst und dass der Platz auf Ihrer 500-GB-Festplatte allmählich knapp wird. Nun möchten Sie eine weitere Festplatte kaufen, aber die vorhandene Ordnerstruktur ist so schön durchorganisiert und Sie möchten das nicht aufgeben. Alle Daten auf die neue Festplatte umkopieren möchten Sie jedoch auch nicht.

Nach der Installation der neuen Festplatte können Sie die Primärpartition (oder ein logisches Laufwerk) als Ordner innerhalb Ihres vorhandenen Ordners DOKUMENTE auf dem Laufwerk `C:` bereitstellen (beispielsweise als `C:\Benutzer\Mike\Meine Bilder`). Einen Laufwerksbuchstaben besitzt die neue Festplatte nicht (obwohl Sie ihr einen zuweisen könnten, wenn Sie das möchten). Legen Sie Ihre Dateien einfach im Ordner MEINE BILDER ab, um das neue Laufwerk zu verwenden. Sie werden dann auf der zweiten Festplatte gespeichert, nicht auf der alten 500-GB-Festplatte (Abbildung 9.48). Erstaunlich!

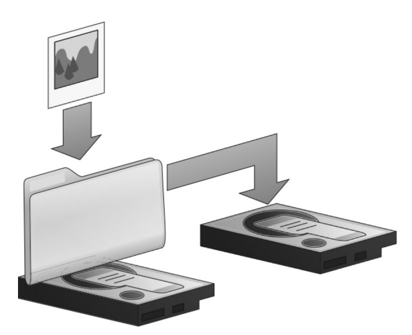


Abb. 9.48: Dem bereitgestellten Ordner hinzugefügte Fotos werden auf der zweiten Festplatte gespeichert.

Um einen Bereitstellungspunkt zu erstellen, klicken Sie einen nicht zugeordneten Bereich einer dynamischen Festplatte mit der rechten Maustaste an und wählen NEUES EINFACHES VOLUME. Der entsprechend benannte Assistent wird gestartet. Im zweiten Dialogfeld können Sie einen Bereitstellungspunkt anstelle eines Laufwerksbuchstabens zuweisen (Abbildung 9.49). Wählen Sie einen leeren Ordner auf einem NTFS-formatierten Laufwerk aus oder legen Sie einen neuen Ordner an, und schon kann es losgehen.

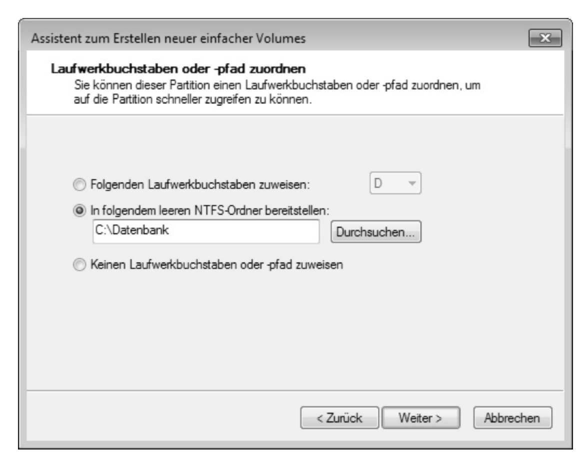


Abb. 9.49: Ein bereitgestellter Datenträger soll erstellt werden

Tipp: Verwendung von dynamischen Datenträgern und Bereitstellungspunkten

Sie werden die elegante Einfachheit der Datenträgerverwaltung erst dann zu schätzen wissen, wenn Sie damit herumexperimentieren. Probieren Sie es also aus! Besorgen Sie sich zwei Laufwerke, installieren Sie diese in Ihrem PC, starten Sie die Datenträgerverwaltung und probieren Sie Folgendes:

1. Erstellen Sie ein gespiegeltes Volume.
2. Erstellen Sie ein Stripesetvolume.
3. Erstellen Sie ein Volume, das sich über beide Laufwerke erstreckt.
4. Erstellen Sie ein Volume, das nur einen Teil eines Laufwerks belegt, und erweitern Sie das Volume dann um einen anderen Teil des Laufwerks. Erweitern Sie das Volume dann um einen Teil des zweiten Laufwerks.
5. Erstellen Sie ein Volume Ihrer Wahl und stellen Sie es dann als Ordner auf dem Laufwerk `C:` bereit.

Nach dem Erstellen der Volumes müssen Sie diese formatieren. Sie können dann sehen, wie sie im Explorer auftauchen. Um neue Volumes einzurichten, müssen sie gelöscht werden. Klicken Sie mit der rechten Maustaste auf ein Volume und wählen Sie VOLUME LÖSCHEN. Es ist fast schon zu einfach.

Wichtig

Manchmal spricht man von der »Aufteilung« von Partitionen. Tatsächlich teilt man sie nicht auf. Wenn Sie aus einer Partition zwei machen möchten, müssen Sie die vorhandene entweder löschen und zwei neue erstellen oder Sie verkleinern die vorhandene Partition und erstellen eine neue mit dem nicht zugewiesenen Speicherplatz. Das ist mit einer Aufteilung gemeint.

Zuweisen und Ändern von Laufwerksbuchstaben und -pfaden

Mit der Datenträgerverwaltung können Sie den Laufwerksbuchstaben, den Laufwerkspfad oder den Bereitstellungspunkt installierter Massenspeichergeräte ändern. Klicken Sie mit der rechten Maustaste

auf ein Laufwerk und wählen Sie LAUFWERKSBUCHSTABEN UND -PFADE ÄNDERN. So können Sie beispielsweise den Laufwerksbuchstaben eines optischen Laufwerks von `D:` auf `Z:` ändern. Oder Sie können für eine Festplatte statt eines Laufwerksbuchstabens einen Bereitstellungspunkt verwenden, damit sie im Explorer als Ordner erscheint. Die Datenträgerverwaltung ist da sehr flexibel.

Wichtig

Die Datenträgerverwaltung ist das Werkzeug der Wahl, um in Windows Laufwerke oder Laufwerksverbunde hinzuzufügen.

9.3.4 Eine Partition formatieren

Im Explorer können Sie jede Windows-Partition bzw. jedes Windows-Volume formatieren. Dazu klicken Sie einfach den Laufwerksnamen mit der rechten Maustaste an und wählen FORMATIEREN (Abbildung 9.50). Sie sehen ein Dialogfeld, in dem Sie nach dem zu verwendenden Dateisystem, der Clustergröße und der Volumebezeichnung gefragt werden. Die Option zur Schnellformatierung weist Windows an, die Cluster nicht zu überprüfen. Das ist praktisch, wenn Sie es eilig haben – und wissen, dass der Datenträger zuverlässig funktioniert.

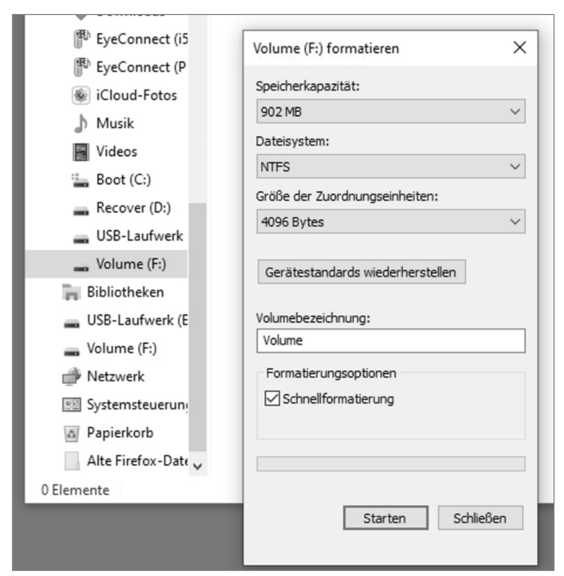


Abb. 9.50: Formatieren einer Partition bzw. eines Laufwerks im Explorer

Bei der Einrichtung von Festplatten benutzt man heute unter Windows bevorzugt die DATENTRÄGERVERWALTUNG, um sie zu formatieren. Wenn Sie ein neues Volume oder eine neue Partition erstellen, fragt Sie der Assistent auch, wie formatiert werden soll. Sofern Sie nicht gerade zu diesen seltsamen Menschen gehören, die sich ein Dual-Boot-System mit irgendeiner alten Windows-Version einrichten wollen, dann sollten Sie immer NTFS verwenden.

Mit allen Installationsmedien von Betriebssystemen können Sie während der Installation Laufwerke partitionieren und formatieren. Windows fordert Sie auf, das Laufwerk zu partitionieren und zu formatieren. Wenn Sie einfach den Anleitungen in den verschiedenen Dialogen folgen, sollte eigentlich nichts schiefgehen.

9.3.5 Speicherplätze

In Windows 8 und neueren Betriebssystemversionen können Sie mit einem oder mehreren physischen Laufwerk(en) beliebiger Größe *Speicherpools* einrichten. Bei den Laufwerken kann es sich um interne HDDs oder SSDs oder um externe per USB angeschlossene Speichergeräte handeln. Das ist ziemlich praktisch. SPEICHERPLÄTZE funktioniert wie ein Werkzeug zur RAID-Verwaltung, nur geht die Funktionalität weit darüber hinaus. Zunächst einmal müssen Sie sich zum Startbildschirm begeben und `Speicherplätze` eintippen. Das Tool taucht dann in den Suchergebnissen auf. Klicken Sie darauf, um das Programm zu starten. Der Startbildschirm bietet im Wesentlichen nur eine Option, nämlich NEUEN POOL UND SPEICHERPLATZ ERSTELLEN (Abbildung 9.51). Wählen Sie diese Option aus.



Abb. 9.51: Startbildschirm von SPEICHERPLÄTZE

SPEICHERPLÄTZE zeigt nun alle verfügbaren installierten und formatierten physischen Laufwerke an und warnt Sie davor, dass sie gelöscht werden, wenn Sie fortfahren (Abbildung 9.52). Wählen Sie die Laufwerke aus, die Sie dem Speicherpool hinzufügen möchten und klicken Sie auf die Schaltfläche POOL ERSTELLEN.

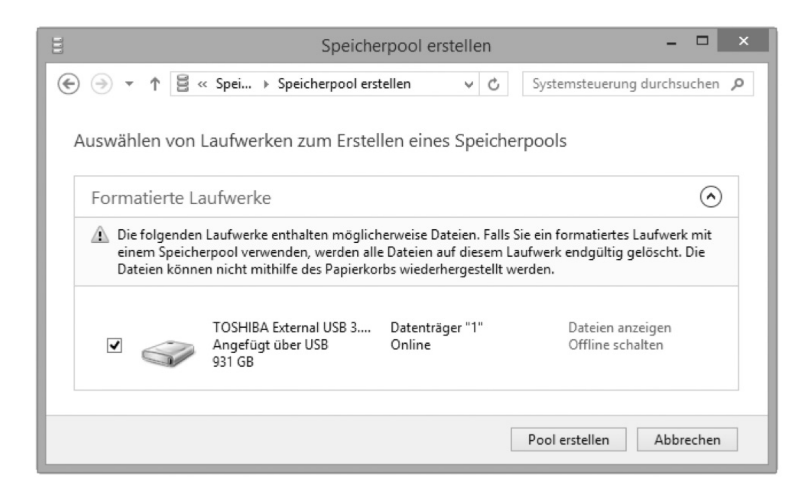


Abb. 9.52: Anzeige der formatierten Laufwerke

Nach dem Erstellen eines Speicherpools müssen Sie den *Resilienztyp* festlegen. Damit ist im Wesentlichen gemeint, wie viele Redundanzebenen verwendet werden, also ob ein oder zwei Laufwerke aus-

fallen dürfen, ohne dass Datenverlust auftritt. Das hört sich doch sehr nach RAID an, oder? Abbildung 9.53 zeigt das Fenster zum Erstellen eines Speicherplatzes mit einer Speicheranordnung, die als *Zwei-Wege-Spiegelung* bezeichnet wird. Hier lässt SPEICHERPLÄTZE andere Werkzeuge zur RAID-Verwaltung einigermaßen alt aussehen.

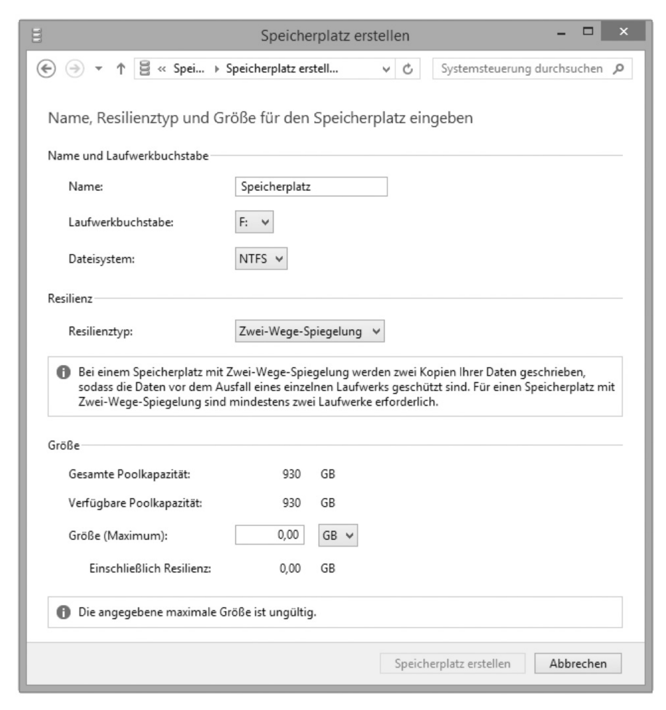


Abb. 9.53: Erstellen eines Speicherplatzes

SPEICHERPLÄTZE bietet drei verschiedene Speicherplatztypen:

- *Einfacher Speicherplatz* ist zusammengelegter Speicher, wie JBOD, bei dem mehrere Laufwerke beliebiger Größe ein einzelnes virtuelles Laufwerk bilden. Einfacher Speicherplatz bietet keine Redundanz, wenn also ein Laufwerk ausfällt, gehen Daten verloren. Dieser Speicherplatztyp eignet sich für temporäre Dateien, Arbeitsdateien und Ähnliches.
- *Gespiegelter Speicherplatz* legt mehr als eine Kopie der Daten an, ähnlich wie ein gespiegeltes RAID, daher kommt es zu keinem Datenverlust, wenn ein Laufwerk ausfällt (oder wenn mehrere Laufwerke ausfallen). Die Anzahl der Laufwerke in diesem Verbund gibt vor, welche Optionen bei der Spiegelung verfügbar sind. Eine Zwei-Wege-Spiegelung erfordert mindestens zwei Laufwerke, für eine Drei-Wege-Spiegelung werden fünf (oder mehr) benötigt. Gespiegelter Speicherplatz funktioniert wie RAID 1 oder RAID 10 und bietet ausgezeichnete Redundanz und hohe Geschwindigkeit.
- *Stabiler Speicherplatz* fügt dem Laufwerksverbund eine weitere Redundanzebene hinzu, ähnlich einem RAID 5 oder RAID 6. Die zusätzliche Redundanz bringt sowohl Vor- als auch Nachteile mit sich. Von Vorteil ist, dass der Speicher effizienter genutzt wird als bei einer Zwei-Wege-Spiegelung, die 20 GB installierten Speicher erfordert, um 10 GB Daten zu speichern. Stabiler Speicherplatz benötigt nur 15 GB installierten Speicher, um 10 GB Daten aufzunehmen. Der Nachteil ist, dass der Verwaltungsaufwand des stabilen Speicherplatzes eine spürbare Auswirkung auf die Geschwindigkeit haben kann. Microsoft empfiehlt, stabilen Speicherplatz für sehr große Dateien zu verwenden, die sich nur selten ändern, beispielsweise für Filmsammlungen. Wenn für den stabilen Speicherplatz drei Laufwerke genutzt werden, kann eines ausfallen, ohne dass es zu Daten-

verlust kommt. Um den Ausfall von zwei Laufwerken ohne Datenverlust zu überstehen, werden (mindestens) sieben Laufwerke benötigt.

Bei einem Laufwerksausfall werden Sie durch das Windows Wartungscenter/Info-Center davon benachrichtigt. Sie können dann SPEICHERPLÄTZE öffnen, um das ausgefallene Laufwerk anzuzeigen und es umgehend ersetzen.

Wichtig

Ein Speicherpool ist eine Zusammenfassung mehrerer physischer Laufwerke, die es Ihnen ermöglicht, die Speicherkapazität flexibel zu erweitern. Speicherplätze sind virtuelle Laufwerke, die aus Speicher bestehen, der nicht Teil eines Speicherpools ist. Speicherplätze verfügen über Redundanz und werden mit einer festen Größe bereitgestellt.

Mit Speicherplätzen wird es möglich, zukünftigen Speicherbedarf vorauszuplanen. Durch *Thin Provisioning* (schlanke Speicherzuweisung) können Sie einen Speicherplatz erstellen, der mehr Speicherkapazität besitzt, als die aktuell vorhandenen physischen Laufwerke bereitstellen. Sie könnten beispielsweise einen Speicherplatz mit Zwei-Wege-Spiegelung anlegen, der aus zwei 2-TB- und einem 3-TB-Laufwerk besteht. Anstatt die Kapazität dieses Speicherplatzes auf 3 TB zu begrenzen, können Sie ihm eine beliebige Größe zuweisen, beispielsweise 12 TB, denn Ihnen ist natürlich klar, dass Ihre Filmsammlung weiter wächst. Wenn Sie die Speicherkapazität der physischen Laufwerke nahezu ausgeschöpft haben, teilt SPEICHERPLÄTZE Ihnen das mit und gestattet es Ihnen, erst dann weitere Speicherkapazität hinzuzufügen. Dank der schlanken Speicherzuweisung brauchen Sie keinen neuen Speicherplatz anzulegen, wenn die Grenze der aktuell vorhandenen Hardware erreicht wird.

Hinweis

Für einige Speicherplatztypen sind SSDs hervorragend geeignet, für andere hingegen gar nicht. Sie können beispielsweise einen Speicherplatz mit Zwei- oder Drei-Wege-Spiegelung anlegen und gewinnen sowohl Geschwindigkeit als auch Redundanz. Wenn Sie hingegen einen stabilen Speicherplatz einrichten, sorgt die interne Funktionsweise von SSDs dafür, dass die Geräte womöglich frühzeitig verschleißen und ausfallen. Verwenden Sie für stabile Speicherplätze am besten nur plattenbasierte Laufwerke.

9.4 Wartung und Fehlerbehebung bei Festplatten

Festplatten sind komplexe mechanische und elektronische Geräte. Da die Festplatten einige Tausend Mal je Minute rotieren, erzeugen sie auch Wärme und Vibrationen. Diese Faktoren sorgen dafür, dass Festplatten vergleichsweise fehleranfällig sind. In diesem Abschnitt werden Sie die grundlegenden Wartungsmaßnahmen kennenlernen, mit denen sich dafür sorgen lässt, dass Festplatten in gutem Zustand bleiben, und erfahren, was Sie tun können, wenn Festplatten tatsächlich komplett ausfallen und möglicherweise repariert werden müssen.

Hinweis

Dieser Abschnitt bezieht sich vornehmlich auf plattenbasierte Laufwerke (HDDs), nicht auf Solid-State-Laufwerke (SSDs). Die auf SSDs anwendbaren Teile sind an den entsprechenden Stellen eingestreut.

9.4.1 Wartung

Die Festplattenwartung umfasst zwei verschiedene Funktionen: das gelegentliche Durchsuchen der Festplatte nach defekten Clustern (Zuordnungseinheiten) und die Organisation des Laufwerks bzw. der gespeicherten Daten, damit schnell darauf zugegriffen werden kann.

Fehlerüberprüfung

Manchmal gehen einzelne Cluster auf Festplatten kaputt. Sie können nichts dagegen tun, deshalb ist es wichtig, dass Sie Festplatten regelmäßig nach defekten Clustern durchsuchen. Meist wird in diesem Zusammenhang von der *Fehlerüberprüfung* gesprochen, zuweilen fällt aber auch noch der Name des älteren Microsoft-Programms *CHKDSK* (*Check Disk*). CHKDSK ist ein Kommandozeilenprogramm. In aktuellen Windows-Versionen gibt es ein Programm mit grafischer Benutzeroberfläche, das Microsoft *Fehlerüberprüfung* nennt. macOS verwendet das *Festplattendienstprogramm*. Linux bietet ein Kommandozeilenprogramm namens `fsck`. Egal, welchen Namen das Programm auch trägt, es erledigt immer dieselbe Aufgabe: Wenn es fehlerhafte Cluster findet, kennzeichnet es diese (mit dem Wert 0000FFF7 in der FAT/MFT), damit das System keine Daten mehr dort abzulegen versucht.

Wichtig

Die CompTIA-Lernziele erwähnen CHKDSK, nicht aber die Fehlerüberprüfung. Sie sollten dennoch mit einer Frage zur Fehlerüberprüfung rechnen.

Die meisten Werkzeuge für die Dateisystemprüfung machen sehr viel mehr, als nur nach fehlerhaften Clustern zu suchen. Sie durchlaufen alle Dateinamen auf dem Laufwerk, suchen nach ungültigen Namen und versuchen, diese zu korrigieren. Sie suchen nach Clustern, denen keine Dateinamen zugeordnet sind (sogenannte *verlorene Ketten*), und löschen sie. Hin und wieder gehen die Verknüpfungen zwischen über- und untergeordneten Ordnern verloren, deshalb überprüft ein gutes Werkzeug für die Fehlersuche alle über- und untergeordneten Ordner. Bei einem Ordner wie etwa `C:\TEST\DATA` stellen sie sicher, dass der Ordner `DATA` korrekt seinem übergeordneten Ordner `C:\TEST` zugeordnet ist, und dass `C:\TEST` korrekt seinem untergeordneten Ordner `C:\TEST\DATA` zugeordnet ist.

Um unter Windows auf die Fehlerüberprüfung zuzugreifen, öffnen Sie den Explorer, klicken das zu überprüfende Laufwerk mit der rechten Maustaste an und wählen im Kontextmenü EIGENSCHAFTEN, um das entsprechende Dialogfeld für das Laufwerk zu öffnen. Aktivieren Sie die Registerkarte TOOLS und klicken Sie auf die Schaltfläche JETZT PRÜFEN (Abbildung 9.54).



Abb. 9.54: Die Registerkarte TOOLS im Dialogfeld EIGENSCHAFTEN

In macOS finden Sie das FESTPLATTENDIENSTPROGRAMM im Ordner DIENSTPROGRAMME, der sich wiederum im Ordner PROGRAMME befindet. Nach dem Öffnen finden Sie verschiedene Optionen, wie Löschen, Partitionieren oder *Erste Hilfe*. Abbildung 9.55 zeigt die für ein Laufwerk verfügbaren Optionen, das kein Startlaufwerk ist. Mit Letzterem können Sie ein Laufwerk auf Fehler überprüfen und gegebenenfalls reparieren. Das Startlaufwerk können Sie bei laufendem macOS zwar überprüfen, aber nicht reparieren. Um es zu reparieren, müssen Sie temporär von der Recovery-Partition starten, die Apple *Wiederherstellungsvolume* nennt. Starten Sie den Rechner neu und halten Sie die Tastenkombination ⌘ + R gedrückt. Dort können Sie dann das Startlaufwerk reparieren.

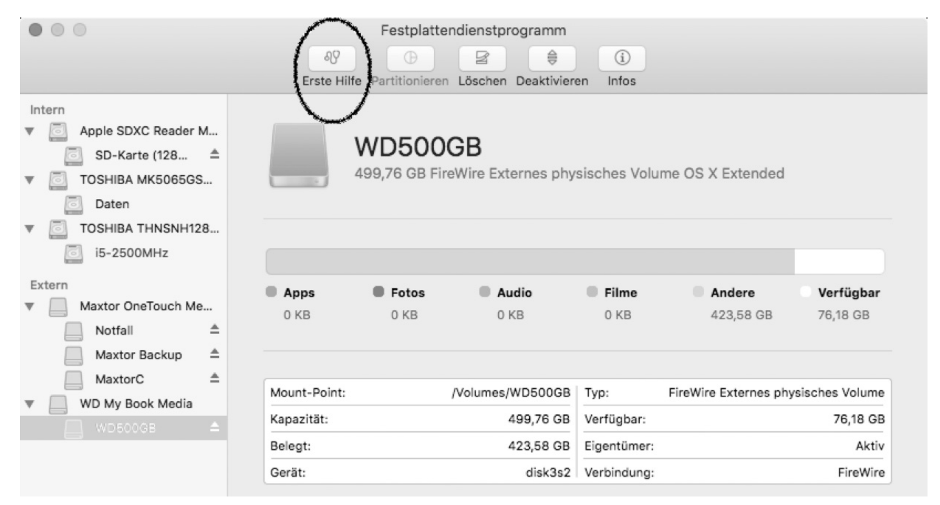


Abb. 9.55: Optionen im Festplattendienstprogramm

Nachdem Sie wissen, wie Sie Datenträger überprüfen lassen können, lautet Ihre nächste Frage wahrscheinlich, wie oft Sie diese prüfen lassen sollten. Ein sinnvoller Wartungsplan sieht eine wöchentliche Ausführung vor. Die Überprüfung geht schnell, und sie ist wirklich bestens geeignet, Ihr System in Topform zu halten. Gleiches gilt für macOS und das Festplattendienstprogramm. Viele Linux-Distributionen führen das Programm `fsck` regelmäßig automatisch aus, daher brauchen Sie sich um nichts weiter zu kümmern.

Defragmentierung

Die Defragmentierung wurde in diesem Kapitel schon kurz erwähnt. Durch fragmentierte (unzusammenhängend gespeicherte) Cluster kann sich die zum Laden von Dateien benötigte Zeit gravierend erhöhen. Sie sollten die Defragmentierung Ihrer Laufwerke zum Teil der monatlich stattfindenden Wartungsarbeiten machen. Das Defragmentierungswerkzeug erreichen Sie auf demselben Weg wie die Fehlerüberprüfung. Klicken Sie im Explorer ein Laufwerk mit der rechten Maustaste an und wählen Sie im Kontextmenü EIGENSCHAFTEN. Auf der Registerkarte TOOLS klicken Sie dann allerdings die Schaltfläche JETZT DEFRAGMENTIEREN an, um das entsprechende Programm zu starten (Abbildung 9.56).

Die Defragmentierung zu beobachten, ist genau einmal interessant. Danach sollten Sie diese jeweils nachts ausführen lassen. Sie sollten Ihre Laufwerke etwa einmal im Monat defragmentieren, aber Sie können das natürlich auch wöchentlich machen. Und wenn sie jede Nacht ausgeführt wird, dauert sie auch nur noch ein paar Minuten. Je mehr Zeit zwischen zwei Defragmentierungsvorgängen liegt, desto länger dauert es. In Windows 7 und neueren Windows-Versionen hat Microsoft die Defragmentierung von HDDs weiter vereinfacht, die nun einmal wöchentlich automatisch stattfindet. Sie können diesen Zeitplan anpassen oder vollständig deaktivieren, aber wenn Sie Ihre Festplatten nicht defragmentieren lassen, dann wird das System mit der Zeit langsamer. Wenn Sie die Fehlerüberprüfung nicht durchführen, verlieren Sie möglicherweise Daten.

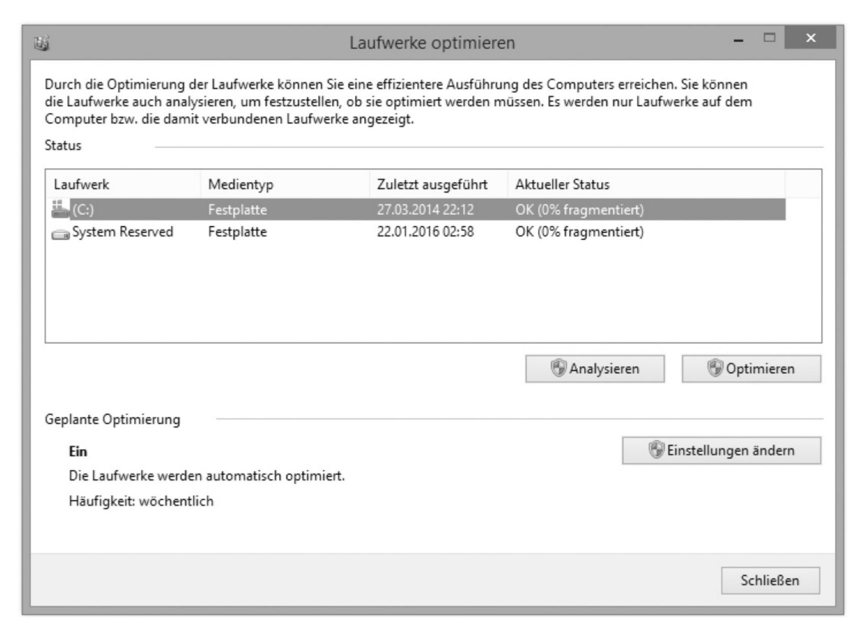


Abb. 9.56: LAUFWERKE OPTIMIEREN, das Defragmentierungswerkzeug von Windows

Hinweis

Falls Sie ein Solid-State-Laufwerk (SSD) einsetzen, brauchen Sie Ihr Laufwerk nicht zu defragmentieren. Tatsächlich sollten Sie SSDs *niemals defragmentieren*, da sich deren Lebensdauer dadurch verkürzt. Windows deaktiviert sogar für SSDs geplante Defragmentierungen automatisch.

Datenträgerbereinigung

Wussten Sie, dass sich auf durchschnittlichen Festplatten Unmengen an Datenmüll ansammelt? Nein, dabei meine ich nicht Daten, die Sie absichtlich auf der Festplatte sammeln, wie z.B. die 23.000 E-Mails, die Sie nicht aus dem E-Mail-Programm löschen wollen. Ich meine hier vielmehr die Dateien, von denen Sie gar nicht merken, dass Windows sie aufbewahrt. Dazu ein paar Beispiele:

- **Dateien im Papierkorb**: Wenn Sie eine Datei löschen, dann wird sie eigentlich gar nicht von der Festplatte entfernt. Sie wird normalerweise vielmehr im PAPIERKORB abgelegt, falls sie später doch einmal benötigt wird. In meinem Papierkorb befinden sich derzeit mehr als 6 GB an Dateien (Abbildung 9.57). Das ist ein ziemlicher Haufen Müll!
- **Temporäre Internetdateien**: Wenn Sie eine Webseite aufsuchen, dann speichert Windows Kopien der Bilder und anderer Elemente auf der lokalen Festplatte, damit die Seite schneller geladen werden kann, wenn Sie erneut darauf zugreifen. (Moderne Browser erledigen das automatisch.)
- **Übertragene Programmdateien**: Auf dem Rechner werden Kopien aller heruntergeladenen Applets gespeichert. Diese Dateien werden angezeigt, wenn Sie im Applet INTERNETOPTIONEN im Register ALLGEMEIN die Schaltfläche EINSTELLUNGEN und anschließend OBJEKTE ANZEIGEN anklicken. Meist handelt es sich dabei aber nur um ein paar winzige Dateien.
- **Temporäre Dateien**: Viele Anwendungen erstellen temporäre Dateien, die normalerweise entfernt werden, wenn die Anwendung beendet wird. Aus dem einen oder anderen Grund werden diese temporären Dateien manchmal nicht gelöscht. Der Speicherort dieser Dateien variiert zwar mit den verschiedenen Windows-Versionen, aber sie befinden sich immer in einem Ordner mit dem Namen `TEMP`.

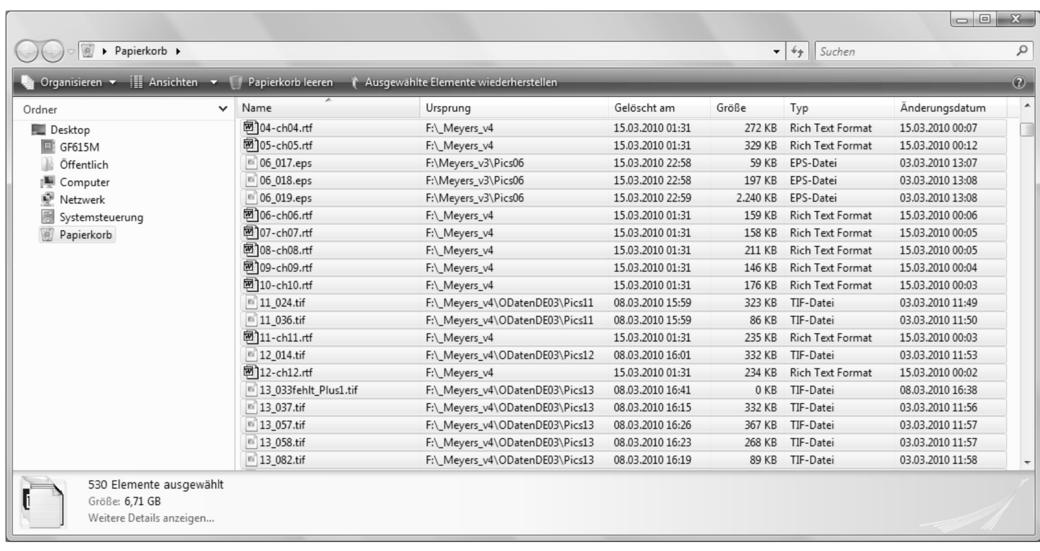


Abb. 9.57: Anzeige des Papierkorbinhalts

Alle Festplatten füllen sich mit der Zeit schließlich mit Unmengen überflüssigen Mülls. Alle Windows-Versionen arbeiten deutlich unzuverlässiger, wenn der Platz auf der Festplatte zur Neige geht. Glücklicherweise gibt es in allen Windows-Versionen ein Programm namens DATENTRÄGERBEREINIGUNG (Abbildung 9.58). Die Datenträgerbereinigung erreichen Sie unter Windows, indem Sie in das Suchfeld `Datenträgerbereinigung` eingeben. Wählen Sie dann in den Suchergebnissen den Treffer aus, um die Datenträgerbereinigung zu starten.

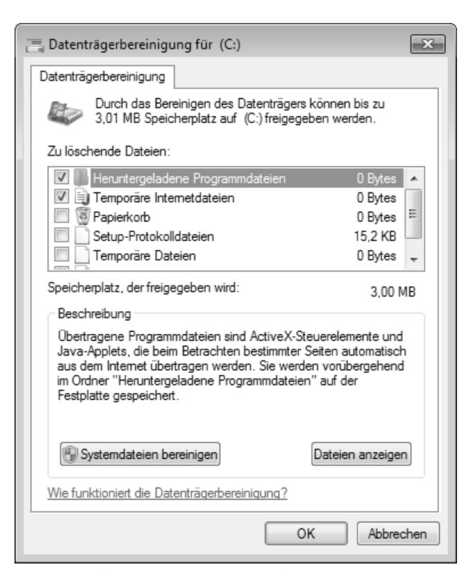


Abb. 9.58: Datenträgerbereinigung

Die Datenträgerbereinigung beseitigt die gerade beschriebenen Dateien (und noch einige weitere). Führen Sie die Datenträgerbereinigung mindestens einmal im Monat aus, um überflüssige Dateien von der Festplatte zu löschen.

Hinweis

macOS und Linux bringen kein Pendant zur Datenträgerbereinigung mit. Es gibt aber Programme von Drittherstellern, wie z.B. BleachBit für Linux, die Vergleichbares leisten.

1001

9.4.2 Fehlerbehebung bei Festplatten

Es gibt kaum schlimmere Probleme als Festplattenfehler. In diesem Abschnitt werden wir uns mit einigen der häufiger im Zusammenhang mit Festplatten auftretenden Fehler und deren Behebung befassen. Die verschiedenen Probleme lassen sich grob vier Kategorien zuordnen: Installationsfehler, beschädigte Daten, »sterbende« Festplattenlaufwerke und RAID-Probleme.

Installationsfehler

Die Installation eines Festplattenlaufwerks und seine Vorbereitung auf das Speichern von Daten erfordert vier verschiedene Schritte: Anschließen, CMOS-Einstellungen, Partitionieren und Formatieren. Wenn Ihnen bei einem dieser Schritte Fehler unterlaufen, wird das Laufwerk nicht funktionieren. Bei einem Fehler können Sie aber jederzeit zum betreffenden Schritt zurückgehen und ihn wiederholen. Da wir uns im Abschnitt zur Problembehebung in Kapitel 8, *Festplattentechnologien*, bereits mit dem physischen Einbau und dem CMOS befasst haben, können wir uns in diesem Abschnitt auf die beiden letzteren Aspekte beschränken.

Partitionierung Partitionierungsfehler fallen generell in zwei Gruppen: Entweder ist überhaupt keine Partition angelegt worden oder die Partition hat die falsche Größe bzw. den falschen Typ. Sie erkennen den ersten Fehlertyp sofort, wenn Sie nach der Installation eines Laufwerks den Explorer öffnen. Wenn Sie die Partitionierung vergessen haben, wird das Laufwerk hier nicht einmal angezeigt, sondern nur in der Datenträgerverwaltung! Wenn Sie die Partition zu klein gemacht haben, wird das schmerzhaft deutlich, wenn Sie beginnen, Dateien darauf zu speichern.

Fehler bei der Partitionierung können Sie beheben, wenn Sie die Datenträgerverwaltung starten und die Partitionierung noch einmal korrekt wiederholen. Klicken Sie einfach nur mit der rechten Maustaste die Partition an und wählen Sie VOLUME ERWEITERN aus, um den Fehler zu korrigieren. Denken Sie aber daran, dass VOLUME LÖSCHEN sämtliche Daten auf dem Laufwerk löscht.

Formatierung Auf unformatierten Festplatten lassen sich keine Daten speichern. Wenn Sie auf ein Laufwerk zugreifen wollen, das nicht formatiert ist, erhalten Sie unter Windows den Fehler »Laufwerk nicht bereit«. Beim Zugriff über die Eingabeaufforderung bekommen Sie außerdem den berühmten Fehler »Unzulässiges Medium«. Formatieren Sie die Festplatte, es sei denn, Sie sind sich sicher, dass sie bereits formatiert war, denn auch beschädigte Dateien können diesen Fehler verursachen. Wenn das Laufwerk bereits formatiert war, lesen Sie in den Abschnitten über beschädigte Daten weiter hinten in diesem Kapitel weiter.

Meist ist das Formatieren ein zeitraubender, langweiliger Vorgang. Manchmal gibt das Laufwerk aber auch schreckliche Geräusche von sich und es werden Fehlermeldungen wie in Abbildung 9.59 angezeigt. Wie Sie wissen, ist *Zuordnungseinheit* eine weitere Bezeichnung für Cluster oder Block.

Das Programm `FORMAT` verwendet den Begriff *Zuordnungseinheit* für Cluster. Das Programm hat einen defekten Cluster entdeckt, den es nun zu reparieren versucht. Früher waren solche Fehler bedeutungslos, weil die damaligen Festplatten grundsätzlich und fertigungsbedingt Fehler aufwiesen. Heute trifft das nicht mehr zu. Moderne Festplatten halten im Hintergrund immer eine Vielzahl zusätzlicher Blöcke bereit, die bei Bedarf automatisch defekte Blöcke ersetzen können. Wenn eine Festplatte viele Fehlermeldungen der Art »Versuch, Zuordnungseinheit Nr. X wiederherzustellen« verursacht, können Sie sicher sein, dass sie bald ihren Geist aufgeben wird und ersetzt werden muss. Besorgen Sie sich die

Diagnosewerkzeuge des Festplattenherstellers, um die Festplatte intensiver zu prüfen. Fehlerhafte Cluster werden von S.M.A.R.T. gemeldet.

```
A:\>format C: /s

ACHTUNG: Alle Daten auf der Festplatte
in Laufwerk C: werden gelöscht!
Formatierung durchführen (J/N)?j


Formatierung 8.056 MB

Versuch, Zuordnungseinheit 37.925 wiederherzustellen
```

Abb. 9.59: Die Fehlermeldung »Versuch, Zuordnungseinheit Nr. X wiederherzustellen«

Bewahren Sie einen kühlen Kopf! Denken Sie bei den erwähnten Fehlern daran, dass es hier immer um neu installierte Festplattenlaufwerke geht. Installationsfehler zeigen sich nicht auf einem System, das seit drei Wochen ordnungsgemäß läuft, sondern dann, wenn Sie ein gerade erst installiertes Laufwerk benutzen wollen. Wenn eine neu installierte Festplatte nicht funktioniert, sollten Sie daher kühlen Kopf bewahren! Spielen Sie den kompletten Installationsvorgang in Gedanken noch einmal durch. Wird die Festplatte von UEFI bzw. im CMOS-Setup automatisch erkannt? Wenn nein, überprüfen Sie alle Daten- und Stromkabel. Wenn die Festplatte jetzt erkannt wird, denken Sie daran, dass sie vielleicht noch partitioniert und formatiert werden muss. Vielleicht muss eine Partition noch aktiviert werden? All dies sind Fragen des gesunden Menschenverstands, die Ihnen wie selbstverständlich einfallen werden, wenn Sie die Installation in Gedanken erneut durchspielen. Auch wenn Sie schon Tausende Festplatten installiert haben, können Ihnen immer noch einfache Fehler wie eine fehlende Stromversorgung unterlaufen. Spielen Sie die Installation dann noch einmal komplett durch. Es hilft wirklich!

Beschädigte Daten

Auf allen Festplatten treten hin und wieder Datenfehler in einzelnen Blöcken auf. Derartige Fehler können Hunderte von Ursachen haben, wie z.B. Spannungsspitzen, versehentliches Abschalten des Systems, beschädigte Installationsmedien oder Computerviren. Meist zeigen sich die entsprechenden Fehler im laufenden Betrieb von Windows. Abbildung 9.60 zeigt ein klassisches Beispiel für diesen Fehlertyp.

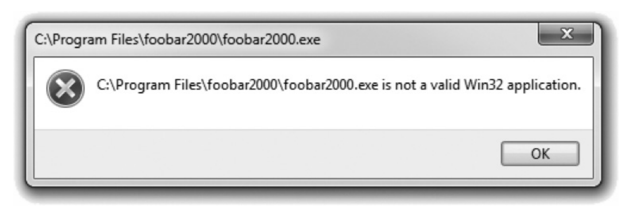


Abb. 9.60: Fehlermeldung wegen beschädigter Daten

Unter Umständen erhalten Sie auch andere Windows-Fehlermeldungen wie diese:

- »Die folgende Datei fehlt oder ist beschädigt«
- »Die Dateiangaben sind falsch oder unvollständig«
- »Datei kann nicht geladen werden«
- »... ist keine gültige Win32-Anwendung«
- »BOOTMGR fehlt ... Drücken Sie Strg-Alt-Entf um neu zu starten«
- »Auf dem PC ist ein Problem aufgetreten. Er muss neu gestartet werden.«
- »Diese App kann auf dem PC nicht ausgeführt werden.«

Wenn wichtige Bootdateien zerstört sind, erhalten Sie beim Booten Textfehlermeldungen, wie die folgenden:

- »Fehler beim Laden des Betriebssystems«
- »Beim Versuch, die Daten der Startkonfiguration zu lesen, ist ein Fehler aufgetreten.«

Die erste Maßnahme bei diesen Problemen besteht in der Ausführung der Datenträgerprüfung. Dann wird der Datenträger untersucht, defekte Bereiche werden markiert und die Daten können hoffentlich in fehlerfreie Cluster verschoben werden. Falls derselbe Fehler nach dem Ausführen der Datenträgerprüfung weiterhin auftritt, ist es sehr wohl möglich, dass auf dem Laufwerk zu viele Blöcke defekt sind und es entsorgt werden muss.

Nahezu alle Festplatten verfügen heute über eine eingebaute *Fehlerkorrektur* (*Error Correction Code* bzw. *ECC*), die die Festplatte laufend überwacht und damit nach defekten Blöcken Ausschau hält. Falls die Fehlerkorrektur einen defekten Block findet, markiert sie ihn in der internen Fehlertabelle des Laufwerks als defekt. Verwechseln Sie diese Fehlertabelle nicht mit der FAT, die bei der Formatierung erstellt wird. Die interne Fehlertabelle der Festplatte wurde im Werk in bestimmten reservierten Bereichen angelegt und ist für das Betriebssystem völlig unsichtbar. Falls die Fehlerkorrektur einen defekten Block findet, wird beim Leseversuch durch den Rechner eine Fehlermeldung angezeigt, die auf den Defekt hinweist. Ein solches Problem kann oft von Datenträgerprüfprogrammen behoben werden.

Ausfallende Festplatten

Physische Festplattenprobleme sind zwar eher selten, haben aber verheerende Folgen, wenn sie denn auftreten. Wenn eine Festplatte wirklich physisch beschädigt ist, dann können normale Servicetechniker nichts mehr retten. Glücklicherweise halten moderne Festplatten eine Menge aus, ohne gleich auszufallen. Die physischen Probleme einer Festplatte sind meist recht offensichtlich: Es treten Schreib- oder Lesefehler auf, das Laufwerk funktioniert zwar noch, macht aber eine Menge Lärm, oder es wird vom Rechner nicht mehr erkannt. In solch einem Fall schlägt möglicherweise schon der nächste Start des Rechners fehl.

Windows meldet Schreib- oder Lesefehler, die bei intakten Festplatten nicht auftreten. Nur kurz vor dem Ableben stehende Laufwerke zeigen ein solches Verhalten.

Alle mechanischen Festplatten machen »Lärm«. Das Summen der rotierenden Festplatten und gelegentliche leicht kratzende Geräusche bei der Positionierung der Schreib/Leseköpfe beim Zugriff auf die Sektoren sind normal. Wenn das Laufwerk aber Geräusche wie die folgenden von sich gibt, dann könnte es langsam den Geist aufgeben:

- Anhaltende, kreischende Geräusche hoher Frequenz
- Mehrmaliges lautes Klicken, kurze Pause und dann wieder mehrmaliges Klicken
- Anhaltende mahlende oder rumpelnde Geräusche

Sichern Sie dann wichtige Daten und ersetzen Sie das Laufwerk. Windows enthält eine Reihe von Hilfsprogrammen für die Datensicherung, aber scheuen Sie sich nicht, nach Lösungen von Drittherstellern zu suchen, wenn sie nicht Ihren Anforderungen entsprechen. Insbesondere die Backup-Lösungen in der Cloud sind eine praktische Option, weil sie nicht nur Ihre Daten sichern, sondern diese zudem an einem externen Ort speichern.

Hinweis

Für die meisten Festplatten gewähren die Hersteller eine dreijährige Garantie. Bevor Sie eine defekte Festplatte entsorgen, sollten Sie auf der Website des Herstellers überprüfen, ob die Garantie schon abgelaufen ist. Sie werden sich wundern, wie oft man kostenlos eine neue, manchmal sogar größere Festplatte erhält. Fragen kostet nichts!

Wenn ein Laufwerk ausfällt, dann merken Sie das schon. Wenn es sich dabei um das Laufwerk mit dem Betriebssystem handelt, dann startet der Rechner nicht mehr. Wenn Sie den Rechner neu zu starten versuchen, dann wird eine Fehlermeldung wie diese angezeigt:

```
No Boot Device Present
```

Wenn es sich um ein zusätzliches Laufwerk handelt, dann wird es einfach im Windows-Explorer nicht mehr angezeigt. Rufen Sie dann zunächst das BIOS-Setup auf und prüfen Sie dort, ob die Einstellungen korrekt sind und ob das Laufwerk automatisch erkannt wird. Wird es angezeigt, dann liegt kein physisches Problem mit dem Laufwerk vor. Wird es nicht angezeigt, dann schalten Sie das System ab und entfernen das Datenkabel, lassen aber das Stromkabel angeschlossen. Starten Sie das System neu und horchen Sie, ob das Laufwerk Geräusche von sich gibt. Wenn der Motor des Laufwerks hochdreht, dann wird das Laufwerk zumindest mit Strom versorgt. In den meisten Fällen weist dies darauf hin, dass das Laufwerk wahrscheinlich noch in Ordnung ist. Dann wenden Sie sich anderen Problemen, wie z.B. nicht richtig angeschlossenem Datenkabel oder falsch gesetzten Jumpern zu. Wenn der Motor nicht anläuft, dann probieren Sie einen anderen Stromstecker aus. Wenn das Laufwerk anschließend immer noch nicht anläuft und Sie (nur bei PATA) die Jumper und das Datenkabel mehrfach überprüft haben, dann gibt es wahrscheinlich Probleme mit der integrierten Laufwerkselektronik und das Laufwerk ist ausgefallen.

Falls es sich um eine SSD handelt, verläuft die Fehlersuche ähnlich. Womöglich funktioniert die Stromversorgung nicht, der Controller auf dem Mainboard oder ein Daten- oder Stromkabel ist defekt, oder die Laufwerkselektronik ist beschädigt. Überprüfen Sie zunächst die Stromversorgung und verwenden Sie ein bekanntermaßen funktionierendes Kabel. Probieren Sie danach aus, das Laufwerk mit einem ebenfalls bekanntermaßen funktionierenden Datenkabel am Mainboard anzuschließen, zuerst am ursprünglichen Anschluss, dann an einem anderen. Funktioniert es noch immer nicht, ist das Laufwerk wahrscheinlich defekt. Sie sollten jedoch noch an einem anderen, funktionierenden Computer ausprobieren, ob es von UEFI/BIOS und der Datenträgerverwaltung erkannt wird.

Hinweis

Wenn eine Festplatte ausfällt, auf der sich absolut unverzichtbare Daten befinden, die nicht anderweitig restauriert werden können, dann können Sie sich an Unternehmen wenden, die sich auf derartige Problemfälle spezialisiert haben. Allerdings wird dies recht teuer, denn unter ca. 1.000 Euro geht hier normalerweise gar nichts. Wenn Sie auf die Daten aber angewiesen sind, dann stellen derartige Unternehmen die letzte und einzige Hoffnung dar. Suchen Sie im Web nach »Datenrettung« oder versuchen Sie Ihr Glück in den Gelben Seiten.

RAID-Probleme beheben

Im Großen und Ganzen handelt es sich bei Laufwerksproblemen von RAID-Verbunden um dieselben Schwierigkeiten wie bei einzelnen Festplatten. Manche der Fehler treten jedoch nur bei RAIDs auf und sollen daher kurz erläutert werden.

Laufwerk wird nicht erkannt Wenn Sie ein Hardware-RAID einsetzen und die Firmware zur Konfiguration des Geräts ein Laufwerk nicht erkennt, sollten Sie zunächst die Stromversorgung des betroffenen Laufwerks und dessen Anschluss überprüfen. Insbesondere werden auf Mainboards mit Onboard-RAID-Systemen spezielle Anschlussverbindungen eingesetzt.

RAID funktioniert nicht mehr Wenn eins der Laufwerke in einem RAID-Verbund ausfällt, können je nach RAID-System und RAID-Controller die verschiedensten Dinge geschehen. Bei einem RAID 0, das so mancher PC-Freak zur Beschleunigung des Systemlaufwerks verwendet, ist das Resultat dramatisch. Wenn hier ein Laufwerk ausfällt, wird Ihnen höchstwahrscheinlich ein Blue Screen angezeigt. Ein Neustart des Rechners wird fehlschlagen oder Sie erhalten die Meldung, dass das Betriebssystem nicht gefunden werden kann. Ihre Daten sind verloren, da es bei einem Stripeset (RAID 0) keine Redundanz gibt. Möglicherweise werden Ihnen vor dem Ausfall des Laufwerks Fehlermeldungen angezeigt, die sich auf Schreib- und/oder Lesevorgänge beziehen. macOS zeigt womöglich das sich drehende regenbogenfarbige Scheibchen (*Pinwheel of Death*), wenn ein Laufwerk ausgefallen ist. Falls es keine anderen systembedingten Probleme gibt, wie z.B. zu wenig RAM oder kaum noch Speicherplatz auf der Festplatte, ist es an der Zeit, RAID- oder Festplatten-Diagnosewerkzeuge wie etwa ein Programm zum Auslesen der S.M.A.R.T.-Informationen einzusetzen.

Bei allen anderen RAID-Leveln wird nichts allzu Ungewöhnliches passieren, wenn ein einzelnes Laufwerk ausfällt. Erst beim nächsten Systemstart wird der RAID-Controller (bei einem Hardware-RAID) oder Windows (falls Sie die eingebauten Werkzeuge verwenden) quengeln und Ihnen mitteilen, dass ein Laufwerk ausgefallen ist.

In vielen Fällen wird der Zugriff auf die Inhalte des RAIDs beim Ausfall eines Laufwerks stark verlangsamt. Eine solche Verlangsamung ist ein Hinweis für Sie, im Geräte-Manager oder der Firmware des RAID-Controllers nachzusehen. Manche Laufwerksausfälle führen zu einem Systemabsturz, andere bleiben unbemerkt, bis Sie beim nächsten Hochfahren des Rechners eine Fehlermeldung erhalten.

Warum das RAID nicht mehr funktioniert oder welche Auswirkungen es gibt, spielt im Grunde genommen keine Rolle und die Problembehebung ist einfach. Ersetzen Sie das defekte Laufwerk und stoßen Sie den Neuaufbau des RAID-Verbundes an. Alles wird gut. Wenn Sie herausfinden müssen, *warum* das Laufwerk ausgefallen ist, sollten Sie probieren, die S.M.A.R.T.-Informationen der defekten Festplatte mit einem geeigneten Programm auszulesen. Sofern die Elektronik noch funktioniert, stehen die Chancen nicht schlecht, dass Sie zu einem Ergebnis kommen.

RAID nicht gefunden Unter den Lernzielen der CompTIA A+-Prüfung 220-1001 findet sich der Begriff »RAID nicht gefunden«. Einen solchen Fehler gibt es eigentlich nicht, gemeint ist eine Reihe von Fehlermeldungen, bei denen ein vorhandener RAID-Verbund nicht mehr angezeigt wird. Die Schwierigkeit mit diesen Meldungen besteht darin, dass sie je nach Hersteller und Modell des verwendeten Hardware-RAIDs bzw. der eingesetzten RAID-Software völlig unterschiedlich lauten.

Ein ordnungsgemäß funktionierendes Hardware-RAID wird in der Konfigurationssoftware auch angezeigt. Falls ein solcher RAID-Verbund plötzlich aufhört zu funktionieren und im Konfigurationsprogramm nicht angezeigt wird, haben Sie ein echtes Problem. Es kann sich in diesem Fall sowohl um defekte Laufwerke als auch um einen fehlerhaften Controller handeln. In beiden Fällen muss die schadhafte Komponente ersetzt werden.

Wenn das RAID verschwunden ist, die Laufwerke aber noch angezeigt werden, hat möglicherweise der RAID-Controller selbst den RAID-Verbund deaktiviert. Das kommt in seltenen Fällen vor, in denen der Controller durch diese Maßnahme versucht, Daten zu schützen. Sie sollten jedenfalls zumindest versuchen, unter Verwendung der zum RAID-Controller zugehörigen Werkzeuge, den RAID-Verbund wiederaufzubauen.

Jenseits von A+

Moderne Festplatten verfügen über zahlreiche andere Funktionen, die man kennen sollte, die aber angehende Techniker nicht unbedingt brauchen. Einige der interessanteren sind Programme zur Kontrolle der Rotationsgeschwindigkeit und Festplattenwerkzeuge von Drittanbietern. Wenn Sie den brennenden Wunsch verspüren, wirklich jedes Detail über Festplatten in Erfahrung zu bringen, gibt es wirklich ausgezeichnete Quellen im Internet, wie z.B. `http://storagereview.com`, eine Website, die ausschließlich HDDs und SSDs sowie anderen Massenspeichergeräten wie SANs und NAS-Geräten gewidmet ist.

9.4.3 Partitionierungswerkzeuge von Drittanbietern

Die Datenträgerverwaltung ist ein gutes Werkzeug, in einigen Situationen jedoch nicht ausreichend. Einige wirklich hervorragende Werkzeuge von Drittanbietern auf dem Markt bieten Ihnen unglaubliche Flexibilität und Leistungsfähigkeit, um Ihren Festplattenspeicher ganz nach Ihren jeweiligen Bedürfnissen anzuordnen und umzustellen. Sie alle besitzen interessante und einzigartige Funktionen, aber im Allgemeinen ermöglichen sie Ihnen, Partitionen auf einer Festplatte zu erstellen, zu ändern oder zu löschen, *ohne* die dort abgelegten Programme oder Daten zu zerstören. Klasse! Diese Programme kommen in den CompTIA A+-Prüfungen nicht vor, aber alle PC-Techniker verwenden min-

destens eines von ihnen, deshalb will ich hier zwei der bekanntesten Beispiele vorstellen: Avanquest *Partition Commander Professional* und das quelloffene Werkzeug *GParted* von Linux.

Avanquest bietet zahlreiche ähnliche Produkte an, unter anderem den sehr praktischen Partition Commander Professional. Das Programm unterstützt alle Windows-Versionen und ermöglicht Ihnen, Partitionen zu ändern, ohne dabei Daten zu zerstören. Zu den interessanten Funktionen gehört die Möglichkeit, dynamische Datenträger ohne Datenverlust in eine Basisfestplatte umzuwandeln (was mit Windows-Bordmitteln nicht möglich ist), die Defragmentierung der MFT auf einer NTFS-Partition und das Verschieben nicht genutzten Speicherplatzes von einer Partition in eine andere auf demselben physischen Laufwerk, wobei die Größe der Partitionen abhängig vom verschobenen Speicherplatz automatisch angepasst wird. Abbildung 9.61 zeigt das Dialogfeld des Partition Commanders zum Verschieben nicht genutzten Speicherplatzes zwischen den Partitionen.

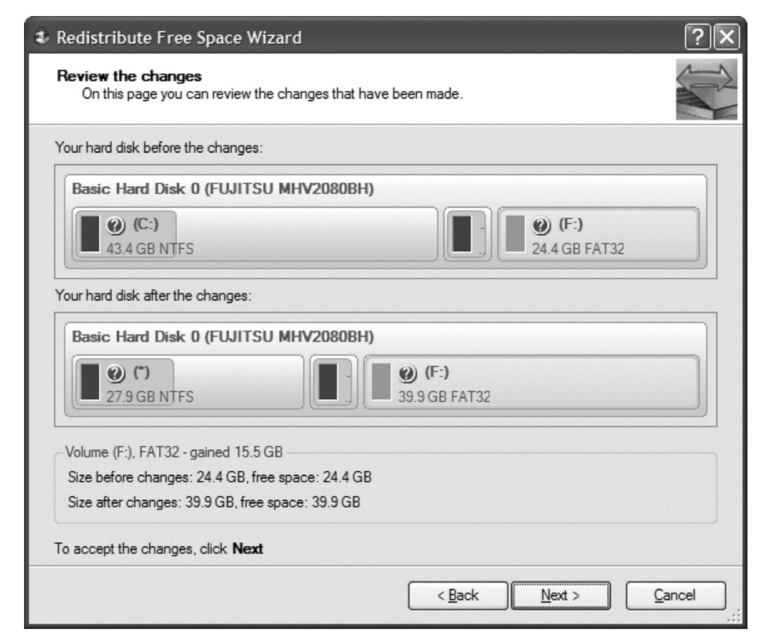


Abb. 9.61: Partition Commander

Das einzige Problem beim Partition Commander besteht darin, dass er Geld kostet. Es ist natürlich nicht verkehrt, für ein gutes Produkt zu bezahlen, aber wenn Sie etwas finden, das die Aufgaben kostenlos erledigt, können Sie es zumindest ausprobieren. In diesem Fall probieren Sie es mit dem *Gnome Partition Editor*, besser bekannt unter dem Namen *GParted*. Sie finden ihn unter `http://gparted.org`.

GParted ist ein unglaublich leistungsfähiger Partitionierungseditor und kann fast alles, was die kostenpflichtigen Editoren auch können, ist aber kostenlos. Möglicherweise haben Sie sogar schon eine Version davon bei sich herumliegen (in Form einer Ubuntu-Live-CD). Wenn Sie sich Abbildung 9.62 genauer ansehen, erkennen Sie, dass er seltsame Namen für die Partitionen verwendet, wie etwa SDA1 oder HDA2. Dabei handelt es sich jedoch um Linux-Konventionen, die alle in der GParted-Hilfe gut dokumentiert sind. Probieren Sie GParted aus, Sie werden es ebenfalls mögen.

Der einzige Nachteil von GParted ist, dass es sich dabei um ein Linux-Programm handelt. Weil es keine Windows-Version gibt, müssen Sie es unter Linux ausführen. Aber wie kann man Linux auf einem Windows-System ausführen, ohne es auf der Festplatte zu installieren? Die Antwort ist einfach: Die Entwickler stellen auch die Werkzeuge zur Verfügung, um eine Live-CD zu brennen, von der Linux gebootet werden kann, um GParted auszuführen.

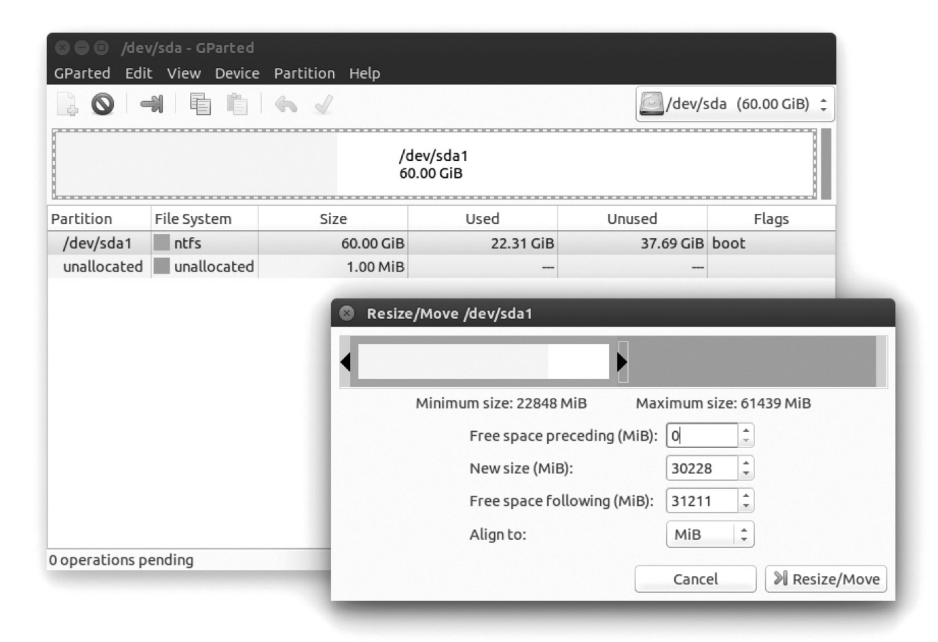


Abb. 9.62: GParted

Eine Live-CD ist ein komplettes Betriebssystem auf einer CD. Es ist jedoch keine Installations-CD wie Ihre Windows-Installations-CD. Das Betriebssystem ist auf der CD bereits installiert. Sie booten von der Live-CD und das Betriebssystem wird in den Arbeitsspeicher geladen, so wie das Betriebssystem von Ihrer Festplatte beim Booten in den Arbeitsspeicher geladen wird. Beim Booten der Live-CD erkennt diese Ihre Hardware und lädt die richtigen Treiber in das RAM, sodass alles funktioniert. Sie erhalten alles, was Sie von einem Betriebssystem erwarten, mit einer großen Ausnahme: Die Live-CD verändert nichts an Ihrer Festplatte. Natürlich können Sie Programme damit ausführen (wie etwa GParted), die mit Ihrer Festplatte arbeiten, weshalb Live-CDs so beliebt bei PC-Technikern sind, weil sie genutzt werden können, um sich in ein launisches System einzuklinken und Programme darauf auszuführen.

Hinweis

Sie können GPartedLive auch auf einem USB-Speicherstick oder auf einer CD-R installieren. Zur Installation sind ein paar Schritte mehr erforderlich, aber Sie kommen in den Genuss einer startfähigen Linux-Version mit einem leistungsfähigen Partitionierungswerkzeug in einem kompakten Format. Eine ausführliche Anleitung finden Sie bei SourceForge unter `https://gparted.sourceforge.io/livecd.php`.

Wahrlich tollkühne Abenteurer könnten auch die *UBCD* (*The Ultimate Boot CD*) verwenden, die einen riesigen Berg praktischer Freeware-Programme enthält, die vom frustrierten Techniker Ben Burrows zusammengetragen wurden, der einmal keine Boot-CD fand, als er sie dringend benötigte. Seine Website finden Sie unter `http://www.ultimatebootcd.com`. Die UBCD enthält mehr als 100 unterschiedliche Werkzeuge, die alle auf einer einzigen Live-CD untergebracht sind. Sie enthält Lowlevel-Diagnosewerkzeuge für alle Festplattenhersteller, mehrere verschiedene Partitionierungswerkzeuge, Programme zum Auslesen der S.M.A.R.T.-Informationen sowie Programme zum Löschen und Klonen der Festplatte (praktisch, wenn Sie eine Festplatte durch eine größere Festplatte ersetzen wollen). Die Programme sind allerdings nur schlecht dokumentiert, und für viele der Werkzeuge benötigen Sie Erfahrungen, die über den Rahmen der CompTIA A+-Prüfungen hinausgehen. Ich darf Ihnen aber sagen, dass ich eine Kopie dieser CD besitze und sie auch nutze.

9.5 Wiederholung

9.5.1 Fragen

1. Welches ist die vollständigste Liste von Dateisystemen, die Windows nutzen kann?
   A. FAT32, NTFS
   B. FAT32, exFAT, NTFS
   C. FAT32
   D. NTFS
2. Wie lassen sich die vier möglichen Einträge in einer Dateizuordnungstabelle korrekt beschreiben?
   A. Dateiname, Datum, Zeit, Größe
   B. Nummer des Anfangsclusters, Nummer des Endclusters, Anzahl der benutzten Cluster, Anzahl der verfügbaren Cluster
   C. Ein Dateiendezeichen, eine Kennung für fehlerhafte Blöcke, ein Code, der anzeigt, dass der Cluster verfügbar ist, die Nummer des Clusters, in dem der nächste Teil der Datei abgelegt ist
   D. Dateiname, Ordnerposition, Nummer des Anfangsclusters, Nummer des Endclusters
3. Welches Programm stellt Microsoft in Windows zur Partitionierung und Formatierung eines Laufwerks bereit?
   A. Formatierung
   B. Datenträgerverwaltung
   C. Datenträgeradministrator
   D. System Commander
4. Was verwendet NTFS, um für die Sicherheit einzelner Dateien und Ordner zu sorgen?
   A. Dynamische Festplatten
   B. ECC
   C. Zugriffssteuerungsliste
   D. MFT
5. Pauline will ihre Festplatte auf Fehler überprüfen. Welches Werkzeug sollte sie in Windows 8.1 dafür verwenden?
   A. FDISK
   B. Format
   C. Datenträgerverwaltung
   D. Fehlerüberprüfung
6. Was verwenden Sie, um Ihre Dateien für andere Benutzer unlesbar zu machen?
   A. Clustering
   B. Komprimierung
   C. Festplatten-Kontingente
   D. Verschlüsselung
7. Wie lässt sich die Kapazität eines NTFS-Laufwerks effizient erweitern?
   A. Sie legen eine erweiterte Partition an, um die Kapazität zu erweitern.
   B. Sie installieren ein zweites Laufwerk und stellen es als Ordner auf dem ursprünglichen kleineren NTFS-Laufwerk bereit.
   C. Sie wandeln das Laufwerk in einen dynamischen Datenträger um und spiegeln es.
   D. Sie formatieren die Festplatte mit der Schnellformatierungsoption.

8. Welche Datenträgerkonfiguration erfordert drei Volumes gleicher Größe?
   A. RAID 5
   B. Gespiegelte Datenträger
   C. Übergreifendes Volume
   D. Stripesetvolume
9. Welches Partitionierungsschema ermöglicht das Anlegen von mehr als vier Partitionen oder Volumes auf einer einzelnen Festplatte? (Wählen Sie zwei Antworten aus.)
   A. MBR
   B. GPT
   C. Dynamischer Datenträger
   D. MFT
10. Welcher Speicherplatztyp mit zwei Laufwerken stellt in Windows 8 oder neueren Windows-Versionen den besten Kompromiss zwischen Redundanz und Geschwindigkeit dar?
    A. Einfacher Speicherplatz
    B. Speicherplatz mit Zwei-Wege-Spiegelung
    C. Speicherplatz mit Drei-Wege-Spiegelung
    D. Stabiler Speicherplatz

9.5.2 Antworten

1. **B.** Moderne Windows-Versionen können FAT32 und NTFS für Festplatten und exFAT für USB-Speichersticks nutzen.
2. **C.** Die vier möglichen Einträge in eine Dateizuordnungstabelle sind ein Dateiendezeichen, eine Kennung für fehlerhafte Blöcke, ein Code, der anzeigt, dass der Cluster verfügbar ist und die Nummer des Clusters, in dem der nächste Teil der Datei abgelegt ist.
3. **B.** In Windows wird die Datenträgerverwaltung zum Partitionieren und Formatieren von Laufwerken genutzt.
4. **C.** Da NTFS einzelne Dateien und Ordner als Objekte betrachtet, kann es über eine Zugriffssteuerungsliste (ACL – Access Control List) für deren Sicherheit sorgen.
5. **D.** Die Fehlerüberprüfung wird verwendet, um ein Laufwerk auf Fehler zu überprüfen.
6. **D.** Um Ihre Dateien unlesbar für andere zu machen, verwenden Sie die Verschlüsselung.
7. **B.** Sie können die Kapazität eines NTFS-Laufwerks effizient erweitern, wenn Sie ein zweites Laufwerk installieren und es auf dem ursprünglichen kleineren NTFS-Laufwerk als Ordner bereitstellen.
8. **A.** RAID 5 erfordert (mindestens) drei Volumes gleicher Größe.
9. **B, C.** Sowohl GPT als auch dynamische Datenträger erlauben das Anlegen von mehr als vier Partitionen oder Volumes auf einer einzigen Festplatte.
10. **B.** Ein Speicherplatz mit Zwei-Wege-Spiegelung verwendet zwei Laufwerke, um Redundanz zu erzielen. Ein einfacher Speicherplatz bietet keine Redundanz und die anderen Antwortmöglichkeiten benötigen drei oder mehr Laufwerke.

Eingabe/Ausgabe 10

Themen in diesem Kapitel:

- Gängige Ein-/Ausgabeanschlüsse warten
- Die verschiedenen Standard-Ein-/Ausgabegeräte und deren Installation
- Funktionsweise und Installation von Speichergeräten (außer HDDs und SSDs) und Wechseldatenträgern

Moderne Computer unterstützen eine Vielzahl von Peripheriegeräten – Ein- und Ausgabegeräte, die an der Systemeinheit angeschlossen werden –, mit denen sich die Funktionalität erweitern und verbessern lässt. In diesem Kapitel sehen wir uns zunächst die gängigen Ein-/Ausgabeanschlüsse an und betrachten dann die dazugehörigen Peripheriegeräte. Das Kapitel endet mit der Vorstellung verschiedener Massenspeichergeräte, wie Flash-Speicherlaufwerke und den zwar immer weniger gebräuchlichen, aber noch nicht ganz ausgestorbenen optischen Medien.

1001

10.1 Allgemeine Ein-/Ausgabeanschlüsse

Immer wenn Sie es mit einem Ein-/Ausgabegerät zu tun bekommen, das sich seltsam verhält, sollten Sie daran denken, dass Sie es nicht nur mit einem Gerät, sondern auch mit dessen Anschluss zu tun haben. Bevor Sie sich den Ein-/Ausgabegeräten zuwenden können, müssen Sie sich erst einmal mit den Aspekten und Technologien einiger der gängigsten Ein-/Ausgabeanschlüsse befassen und auch damit, wie Sie dafür sorgen können, dass sie korrekt funktionieren.

10.1.1 Serielle Anschlüsse

Hin und wieder müssen Techniker sich um ältere Geräte kümmern, wie etwa ein installiertes Verkaufssystem oder alte Netzwerkkomponenten, die immer noch ihren Dienst verrichten. Viele dieser alten Geräte verwenden *serielle Anschlüsse* nach dem *Recommended Standard* (empfohlener Standard) 232 oder kurz RS-232, den es schon seit 1960 gibt. Ein serieller Anschluss ist eine D-förmige 9-polige Buchse (männlich), die als DB-9 oder RS-232 bezeichnet wird. Sie werden bei Produkten, die jünger als ein Jahrzehnt sind, keine seriellen Anschlüsse mehr finden, aber die CompTIA hält sie für wichtig genug, um sie in die Lernziele der Prüfung aufzunehmen. Abbildung 10.1 zeigt einen seriellen Stecker mit Kabel und einen DB9-Anschluss.



Abb. 10.1: DB-9-Stecker und Buchse

Wichtig

Sie müssen nicht wissen, wie serielle Anschlüsse funktionieren, um die Prüfung zu bestehen. Sie sollten sich jedoch die Bezeichnung der Buchse und des Steckers (DB-9 und RS-232) merken.

10.1.2 USB-Anschlüsse

Fast alle nur erdenklichen Gerätetypen werden über den *Universal Serial Bus* (USB) angeschlossen. Hier folgt eine eingehendere Betrachtung von USB aus der Perspektive des Technikers und einiger der Probleme, die bei der Verwendung von USB-Geräten auftreten können.

USB-Grundlagen

Den Eckpfeiler einer USB-Verbindung bildet der *USB-Host-Controller*, ein Schaltkreis, der normalerweise in den Chipsatz eingebaut ist, der alle daran angeschlossenen USB-Geräte steuert. Innerhalb des Host-Controllers befindet sich mit dem *USB-Root-Hub* jener Teil des Host-Controllers, der die physische Verbindung mit den USB-Anschlüssen herstellt. Ein USB-Root-Hub ist eigentlich auch nur ein Bus, der dem Erweiterungsbus in vielerlei Hinsicht ähnelt. Abbildung 10.2 zeigt eine Skizze der Beziehungen zwischen Host-Controller, Root-Hub und USB-Anschlüssen.

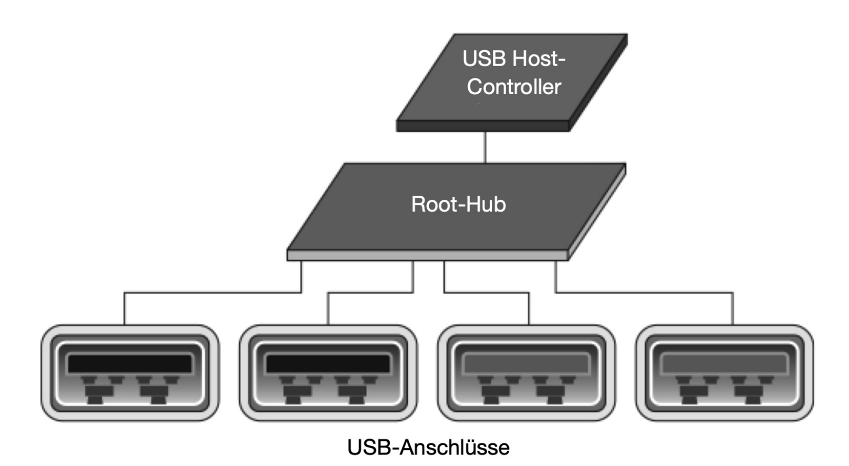


Abb. 10.2: Host-Controller, Root-Hub und USB-Anschlüsse

Ein einzelner Host-Controller unterstützt theoretisch bis zu 127 Geräte, obwohl diese Zahl in der Praxis kaum realistisch ist. Selbst wenn der Host-Adapter eine bestimmte Anzahl von Anschlüssen unterstützt, heißt das noch lange nicht, dass der Mainboard-Hersteller auch so viele Anschlüsse einbaut. Ein typisches Beispiel: Der Chipsatz AMD X370 unterstützt 16 Anschlüsse, aber nur wenige Mainboard-Hersteller stellen so viele Anschlüsse zur Verfügung.

Der USB-Host-Controller ist der *Master* eines jeden Geräts (dem *Slave*), das daran angeschlossen ist. Der Host-Controller sendet Kommandos und versorgt die USB-Geräte mit Strom. Der Host-Controller befindet sich *upstream* und steuert die *downstream* angeschlossenen Geräte (Abbildung 10.3). Alle USB-Geräte, die an einen einzelnen Host-Controller angeschlossen sind, *teilen* sich diesen USB-Bus mit allen anderen daran angeschlossenen Geräten. Deshalb sinkt die Geschwindigkeit und der verfügbare Strom mit jedem weiteren angeschlossenen Gerät.

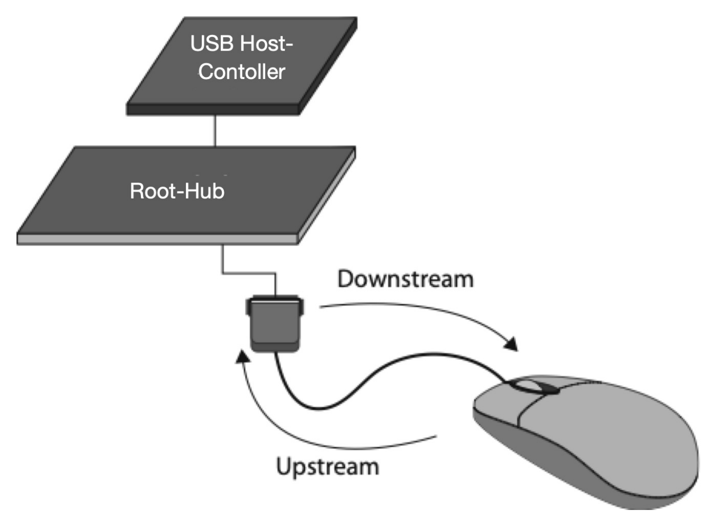


Abb. 10.3: Host-Controller (upstream) und USB-Maus (downstream)

USB-Standards und Kompatibilität

Der USB-Standard ist mehrfach überarbeitet worden und es gibt verschiedene Versionen:

- Die Version 1.1 war der erste weitverbreitete USB-Standard und hat zwei Geschwindigkeiten definiert, *Low-Speed* mit maximal 1,5 Mbps (für Tastaturen und Mäuse mehr als ausreichend) und *Full-Speed* mit bis zu 12 Mbps Transferrate.
- USB 2.0 *Hi-Speed* brachte als Neuerung eine Übertragungsrate von 480 Mbps mit.
- USB 3.0 schafft Geschwindigkeiten von bis zu 5 Gbps – das ist zehnmal schneller als USB 2.0! USB 3.0 wird auch als *SuperSpeed USB* bezeichnet. Manchmal wird es auch *USB 3.1 Gen 1* genannt, allerdings *nicht* in den CompTIA A+-Prüfungen.
- USB 3.1 erreicht Übertragungsraten von bis zu 10 Gbps und wird als *SuperSpeed USB 10 Gbps* oder *USB 3.1 Gen 2* bezeichnet.

Wenn Sie der Ansicht sind, dass diese ganzen Namen und Nummern für Verwirrung sorgen, haben Sie recht. In Tabelle 10.1 sind die verschiedenen USB-Standards daher zusammengefasst.

Name	Standard	Maximale Geschwindigkeit	Typische Anwendung
Low-Speed USB	USB 1.1	1,5 Mbps	Tastaturen, Mäuse
Full-Speed USB	USB 1.1	12 Mbps	Kopfhörer, Bluetooth-Geräte
Hi-Speed USB	USB 2.0	480 Mbps	Webcams, Kartenleser, ältere WLAN-Adapter, ältere USB-Speichersticks
SuperSpeed USB	USB 3.0	5 Gbps	USB-Speichersticks, externe Speichergeräte, WLAN-Adapter
SuperSpeed USB 10 Gbps	USB 3.1 Gen2	10 Gbps	USB-Speichersticks, externe Speichergeräte, Netzwerke

Tabelle 10.1: USB-Standards

Hinweis

Die verschiedenen USB-Standards definieren nicht nur neue Geschwindigkeiten. Viele Low-Speed- und Full-Speed-USB-Geräte entsprechen ebenfalls dem USB-2.0-Standard.

USB 2.0 ist vollständig abwärtskompatibel zu Geräten, die den langsameren USB-1.1-Standards entsprechen, und auch USB 3.0/3.1 ist abwärtskompatibel zu USB-2.0-Geräten. Die alten Geräte laufen dann aber natürlich auch nicht schneller als zuvor. Um die schnellste USB-Geschwindigkeit nutzen zu können, müssen USB-Geräte an USB-Ports angeschlossen werden, die mindestens so schnell wie das Gerät sind. Während die Abwärtskompatibilität Ihnen zumindest erlaubt, ein neueres USB-Gerät an einem älteren Anschluss zu verwenden, müssen Sie nur ein wenig rechnen, um sehr schnell zu erkennen, wie viel Zeit es kostet, wenn man eine 2 GB große Datei nur mit 480 Mbps statt mit 10 Gbps Transferrate überträgt!

Wichtig

Das *USB-IF* (*USB Implementers Forum*) verwendet die Begriffe *Low-Speed* und *Full-Speed* nicht offiziell zur Beschreibung von 1,5- und 12-Mbps-Geräten, sondern spricht nur von »USB 1.1«. Sie werden jedoch feststellen, dass in den CompTIA A+-Prüfungen die marktüblichen Bezeichnungen verwendet werden.

Natürlich wollen die meisten Leute von diesen erstaunlichen Geschwindigkeiten profitieren, aber was soll man machen, wenn es auf dem Mainboard keine SuperSpeed-USB-Anschlüsse gibt? Eine Möglichkeit ist der Einbau einer Steckkarte (Abbildung 10.4).

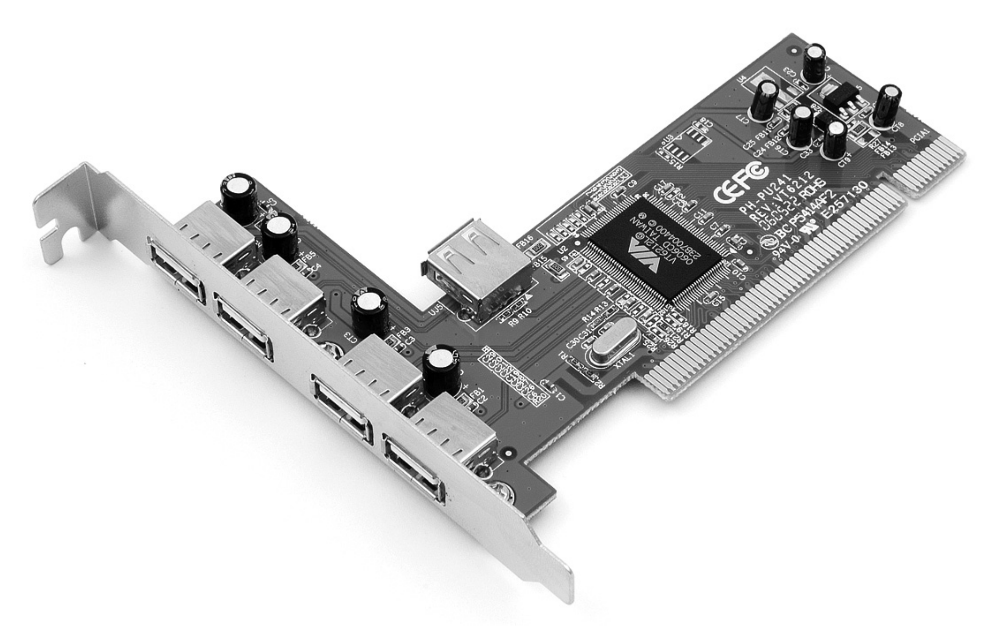


Abb. 10.4: USB-Steckkarte

Mainboards, die sowohl USB 1.1 als auch USB 2.0 unterstützen, teilen sich gewöhnlich die vorhandenen USB-Anschlüsse (Abbildung 10.5). Beim Anschluss eines Low- oder Full-Speed-Geräts übernimmt der USB-1.1-Host-Controller und beim Anschluss eines Hi-Speed-Geräts der USB-2.0-Host-Controller dessen Verwaltung.

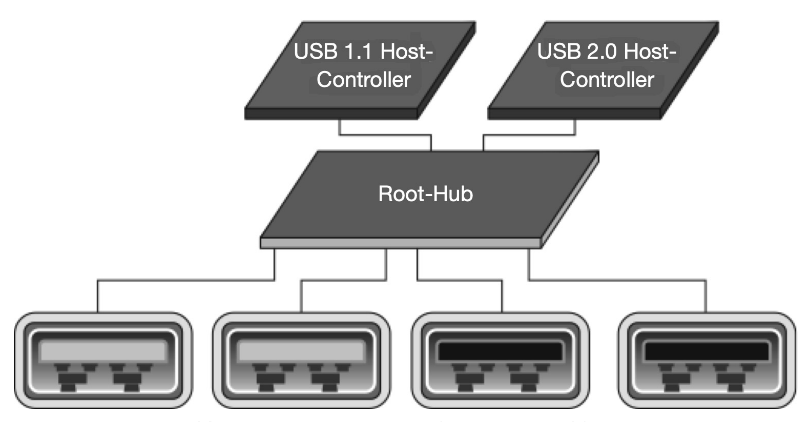


Abb. 10.5: Gemeinsam verwaltete USB-Anschlüsse

USB 3.0 und 3.1 hingegen unterscheiden sich hinreichend deutlich von USB 2.0, sodass dafür eigene Host-Controller verwendet werden. Sie können ältere USB-Geräte an USB-3.0- oder USB-3.1-Anschlüssen betreiben, dabei aber nur die geringere Geschwindigkeit des älteren Standards erzielen. Mit 10 Gbps laufen ausschließlich die Anschlüsse des Standards USB 3.1 (Abbildung 10.6).

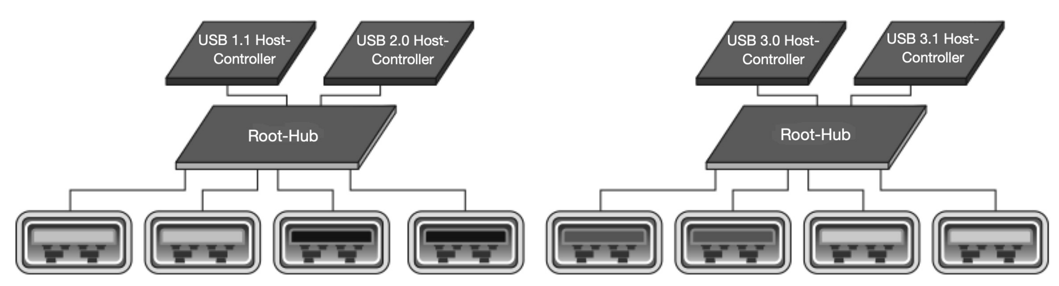


Abb. 10.6: Gemeinsam genutzte USB-Anschlüsse für alle Geschwindigkeiten

USB-Kabel und -Anschlüsse

Als USB 1.1 vorgestellt wurde, legte der Standard zwei Steckertypen fest: USB A und USB B. USB-A-Stecker und -Anschlüsse dienen zur Verbindung mit dem PC. Die meisten Peripheriegeräte verwenden B.

Die Typen A und B gibt es in verschiedenen Größen, neben Standard-USB-A und -B gibt es Mini-A/B und Micro-A/B (Abbildung 10.7). Mini- und Micro-Anschlüsse haben sich kaum verbreitet; die meisten Geräte sind fest verdrahtet. Sie werden vor allem zum Anschluss von Kameras und Smartphones eingesetzt.

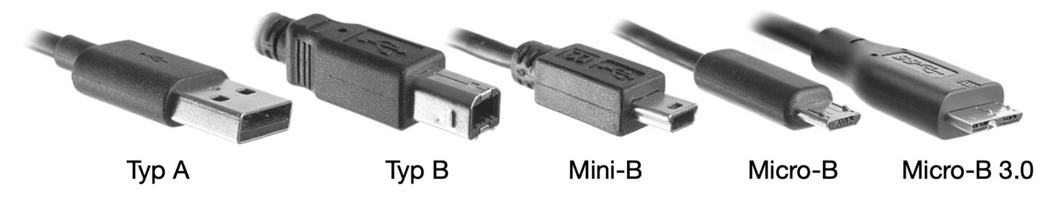


Abb. 10.7: USB-Stecker der Typen A und B

Die Vorstellung von USB 3.0 machte eine Aktualisierung der USB-A- und neue Micro-B-Anschlüsse erforderlich (wie den Stecker ganz rechts in Abbildung 10.7), die mit den größeren Geschwindigkeiten zurechtkommen. Bei USB-1.1- und USB-2.0-Kabel verwenden die Stecker und Anschlüsse A und B vier Pins. Bei USB 3.0/3.1 A und B finden hingegen neun Pins Verwendung. Der USB-3-A-Stecker sieht genauso aus wie der ältere USB-A-Stecker, besitzt jedoch neun Pins.

Wichtig

Die Bezeichnungen der verschiedenen Stecker und Anschlüsse haben sich im Laufe der Zeit geändert. Die ursprünglichen Stecker und Anschlüsse des Typs A werden in der neuesten Spezifikation Standard-A und Standard-B genannt, obwohl die meisten Leute sie als Typ A und Typ B bezeichnen (siehe Abbildung 10.7). Die Mini- und Micro-Versionen werden auch Mini-A, Mini-B, Micro-A, Micro-B und Micro-B 3.0 genannt

Die USB-Hersteller haben ein Farbschema zur Identifizierung der verschiedenen Typen eingeführt (Abbildung 10.8). In Tabelle 10.2 sind die Farben und die Standards aufgeführt.

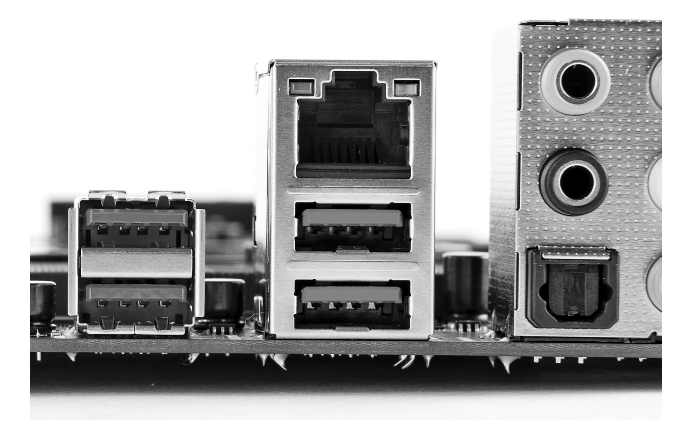


Abb. 10.8: USB-3.0- (links) und USB-3.1-Anschlüsse (Mitte)

USB-Standard	Farbe des Anschlusses
USB 1.1	Weiß
USB 2.0	Schwarz
USB 3.0	Blau
USB 3.1	Türkis

Tabelle 10.2: Farben von USB-Anschlüssen

Hinweis

Es gibt auch Laptops mit roten, orangefarbenen oder gelben USB-Anschlüssen. Dabei handelt es sich um Anschlüsse, die immer spannungsführend sind (um andere Geräte aufzuladen), auch wenn der Laptop ausgeschaltet ist. Einen Standard gibt es für diese Farben aber nicht.

Es hat sich als erstaunlich schwierig erwiesen, USB-Stecker des Typs A richtig herum einzustöpseln. Manche Leute meinen scherzhaft, dass USB-Stecker eigentlich *drei* Orientierungen kennen: nach oben, nach unten – und eine dritte, nämlich diejenige, in der sie endlich passen!

Das USB-IF-Gremium veröffentlichte schließlich den USB-C-Standard, um die Steckertypen zu vereinheitlichen. Außerdem spielt beim Typ C die Ausrichtung des Steckers keine Rolle. USB Typ C soll die A- und B-Stecker aller Größen ersetzen.

Hinweis

Bei den Bezeichnungen der Stecker des Typs C gibt es ein ziemliches Durcheinander, wie schon bei den Typen A und B. Viele Leute verwenden einfach USB-C.

Der Typ C verwendet 24 Pins und die Ausrichtung des Steckers spielt beim Einstecken eine Rolle. Er unterstützt USB 3.1 vollständig und sogar andere Busse, wie etwa Thunderbolt (siehe Abschnitt 10.1.4, *Thunderbolt-Anschlüsse*, später in diesem Kapitel). USB-C ist im Begriff, Micro-USB schnell als dominierenden Anschluss für kleine Geräte abzulösen (siehe Abbildung 10.9).



Abb. 10.9: USB-C-Stecker

Hinweis

Im Allgemeinen wird bei einer USB-Verbindung nur die Geschwindigkeit des langsamsten beteiligten Geräts erreicht. Wenn Sie also ein USB-2.0-Gerät am USB-3.x-Anschluss Ihres PCs betreiben, erreichen Sie nur USB-2.0-Geschwindigkeit.

Die Beschränkung der Kabellänge darf nicht außer Acht gelassen werden. Bei USB 1.1 und USB 2.0 dürfen die Kabel maximal fünf Meter lang sein. Die Kabel der meisten USB-Geräte sind weit entfernt von dieser Grenze, aber einige Geräte, wie etwa Digitalkameras, werden tatsächlich mit so langen Kabeln ausgeliefert. Im USB-3.x-Standard ist keine Beschränkung der Kabellänge spezifiziert. Da es sich bei USB um eine bidirektionale Verbindung handelt, reagieren selbst gut abgeschirmte, verdrillte 0,8-mm-Standardkabel empfindlich auf elektromagnetische Interferenzen. Um diese Probleme zu vermeiden, bleibe ich bei Kabeln von höchstens zwei Metern Länge, außer unter ganz bestimmten Umständen. Unser Fotograf hat seine Kamera beispielsweise mit einem 4,5 Meter langen Kabel an seinen Mac angeschlossen. Im Studio funktioniert das tadellos.

Wichtig

Viele Hersteller bieten verschiedene USB-A/B-Adapter an. Damit können Sie ein reines USB-A-Kabel verwenden, um beispielsweise einen Drucker am PC anzuschließen.

USB-Hubs

Jeder USB-Host-Controller unterstützt bis zu 127 USB-Geräte, aber wie bereits erwähnt, stellen die meisten Mainboard-Hersteller nur sechs oder acht USB-Anschlüsse zur Verfügung. Was also machen Sie, wenn Sie mehr USB-Geräte anschließen wollen, als Anschlüsse auf dem Mainboard vorhanden sind? Sie bauen weitere Host-Controller ein (in Form interner Karten), oder Sie verwenden einen USB-Hub. Ein USB-Hub ist ein Gerät, das einen USB-Anschluss auf zwei oder mehr USB-Anschlüsse

erweitert, und zwar fast immer von einem der an den Root-Hub angeschlossenen USB-Anschlüsse aus. Abbildung 10.10 zeigt einen typischen USB-Hub. USB-Hubs werden manchmal auch in Peripheriegeräte integriert. Der Monitor in Abbildung 10.11 besitzt einen eingebauten USB-Hub – sehr praktisch!



Abb. 10.10: USB-Hub



Abb. 10.11: Monitor mit eingebautem USB-Hub

Hubs gibt es mit (*aktive Hubs*) und ohne eigene Stromversorgung (*passive Hubs*). Wenn Sie einen Mehrzweck-USB-Hub wie den aus Abbildung 10.10 verwenden, dann sollten Sie sich für einen mit eigener Stromversorgung entscheiden, weil die an einem einzelnen USB-Root-Hub angeschlossenen Geräte ansonsten zu viel Energie verbrauchen und die Geschwindigkeit verringern, denn alle Geräte teilen sich den Bus.

USB-Konfiguration

Die größte Herausforderung bei der USB-Fehlersuche hat direkt mit der weiten Verbreitung und der einfachen Nutzung zu tun. Nahezu jeder moderne PC hat mehrere USB-Anschlüsse, und jeder kann sich im Computerladen die allerneuesten USB-Geräte kaufen. Zu Problemen kommt es, wenn die Installationsaktivitäten außer Kontrolle geraten, weil zu viele Geräte die falschen Anschlüsse benutzen oder zu viel Energie benötigen. Glücklicherweise können Sie diese Probleme unter Befolgung einiger einfacher Schritte vermeiden oder ganz aus der Welt schaffen.

Windows, macOS und Linux bringen zahlreiche vorinstallierte Treiber für USB-Geräte mit. Die Betriebssysteme erkennen Tastaturen, Mäuse und andere Basisgeräte zuverlässig. Wenn Ihre neue Maus oder die Tastatur jedoch über irgendwelche Extras verfügt, werden diese von den USB-Stan-

dardtreibern möglicherweise nicht unterstützt. Damit ich auch wirklich alle Funktionen nutzen kann, installiere ich immer die mit dem Gerät gelieferten oder von der Website des Herstellers heruntergeladenen Treiber.

Das letzte und schwierigste Problem betrifft die Stromversorgung. Wenn die für USB-Geräte verfügbare Energie deren Bedarf nicht decken kann, führt das zu Furcht einflößenden Fehlermeldungen und die Geräte funktionieren möglicherweise gar nicht oder nur fehlerhaft. Wird zu viel Strom verbraucht, müssen Sie Geräte vom jeweiligen USB-Root-Hub trennen, bis der Fehler verschwindet. Wenn Sie mehr Geräte anschließen möchten, als Ihr USB-Hub unterstützt, können Sie eine zusätzliche USB-Erweiterungskarte kaufen.

Es gibt ein weiteres Problem mit der USB-Stromversorgung: Manche USB-Geräte gehen in den Ruhezustand über und wachen dann nicht mehr auf. Tatsächlich werden sie vom Betriebssystem in den Ruhezustand versetzt. Das könnte das Problem sein, wenn ein vorher funktionierendes USB-Gerät plötzlich nicht mehr im Geräte-Manager erscheint.

Um den USB-Energieverbrauch unter Windows zu überprüfen, öffnen Sie den Geräte-Manager und suchen unter dem Eintrag USB-CONTROLLER nach USB-Hubs. Klicken Sie den entsprechenden Hub mit der rechten Maustaste an und wählen Sie im Kontextmenü EIGENSCHAFTEN. Anschließend aktivieren Sie die Registerkarte ENERGIEVERWALTUNG und entfernen das Häkchen vor COMPUTER KANN DAS GERÄT AUSSCHALTEN, UM ENERGIE ZU SPAREN (Abbildung 10.12).

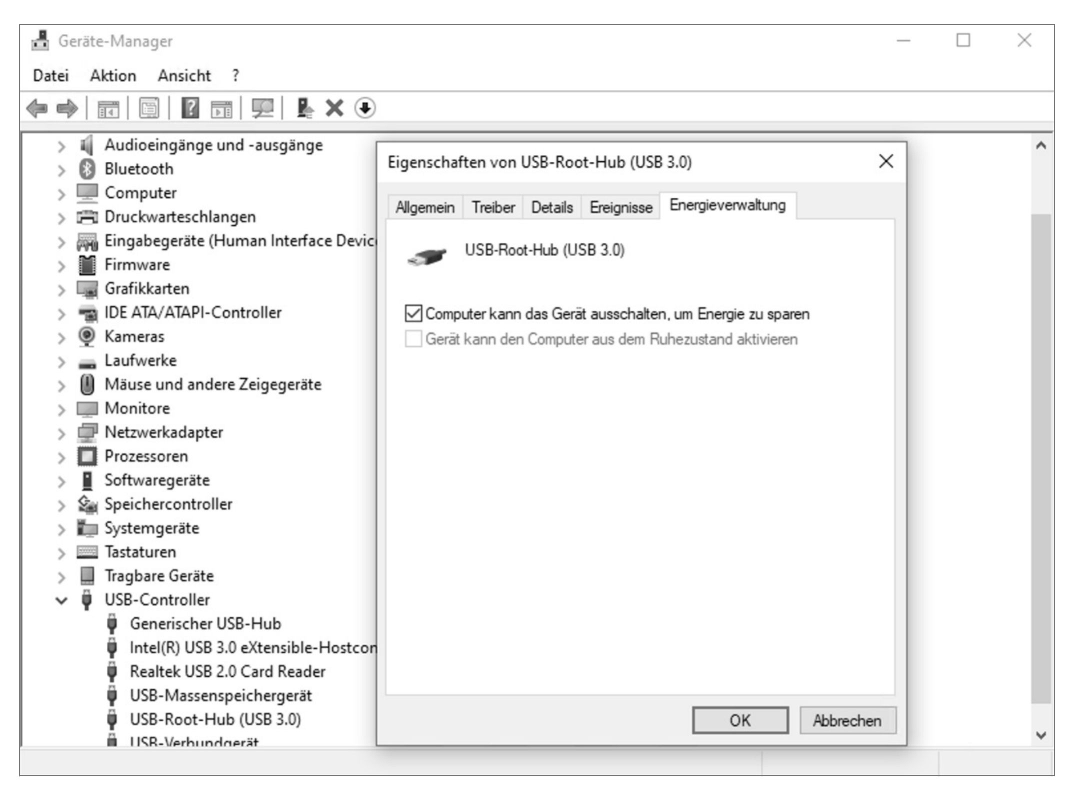


Abb. 10.12: Registerkarte ENERGIEVERWALTUNG für einen USB-Root-Hub

Tipp

Sehen Sie sich auf `http://totalsem.com/100x` die Übung zu Kapitel 10 an, mit der Sie Ihre Kenntnisse der USB-Geschwindigkeiten überprüfen können.

10.1.3 FireWire-Anschlüsse

Auf den ersten Blick ähneln *FireWire*, das auch *IEEE 1394* genannt wird, und USB einander stark. FireWire kann mit denselben Funktionen wie USB glänzen, verwendet aber andere Stecker und ist die ältere der beiden Technologien. FireWire verwendet verschiedene Anschlüsse und Steckertypen für den Anschluss von Geräten wie externen Festplatten oder Camcordern (Abbildung 10.13). Wie bei USB gab es auch bei FireWire mehrere Standards. Der erste Standard IEEE1394a erreichte eine Geschwindigkeit von 400 Mbps, die beim Standard IEEE 1394b auf 800 Mbps erhöht wurde. In der Praxis können Sie gelegentlich noch FireWire-Geräten begegnen, sie werden jedoch zunehmend seltener. FireWire hat eine kurze Hochzeit erlebt, vor allem bei Geräten von Apple, wurde aber inzwischen von Thunderbolt verdrängt.

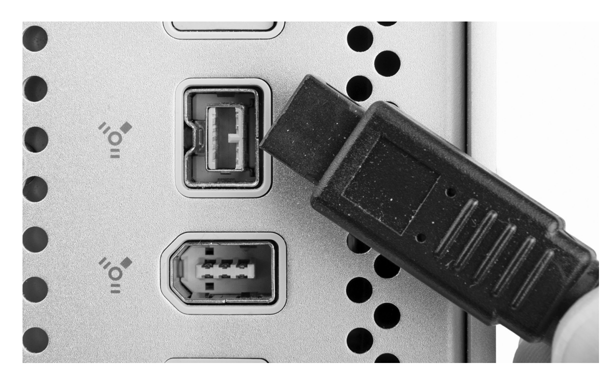


Abb. 10.13: FireWire800-Anschluss und -Stecker über einem FireWire400-Anschluss

10.1.4 Thunderbolt-Anschlüsse

Intel hat *Thunderbolt* als Alternative mit sehr hoher Geschwindigkeit zu vorhandenen Technologien wie USB und FireWire entwickelt. Es nutzt den PCI-Express-Bus, um bis zu sechs externe Peripheriegeräte miteinander zu verbinden. (Heutzutage funktioniert Thunderbolt zusammen mit USB. Die PC-Hersteller haben Thunderbolt schnell übernommen. Inzwischen hat diese Technologie bei vielen Laptop- und Desktop-Systemen Einzug gehalten. Wenn Sie Ihren PC selbst zusammenstellen und ein Thunderbolt-fähiges Mainboard verwenden, können Sie sich eine PCIe-Thunderbolt-Karte kaufen. Thunderbolt unterstützt Videoübertragungen (bis hin zu einem 4K-Monitor, siehe Kapitel 17) und Audiosignale. Auch Massenspeichergeräte funktionieren problemlos.

Bei Thunderbolt 1 und Thunderbolt 2 werden die Geräte über Mini-DisplayPort-Anschlüsse (MDP) miteinander verbunden. Thunderbolt 3 verwendet USB-Stecker des Typs C. Thunderbolt kann sowohl Kupferkabel als auch Glasfaserleitungen nutzen. Kupferkabel dürfen bis zu drei Meter lang sein, Glasfaserleitungen hingegen bis zu 60 Meter.

USB und Thunderbolt verwenden zwar den gleichen Stecker des Typs C, sind aber nicht kompatibel, was die Hersteller veranlasste, ihre Anschlüsse mit deutlich erkennbaren Logos zu kennzeichnen (Abbildung 10.14).

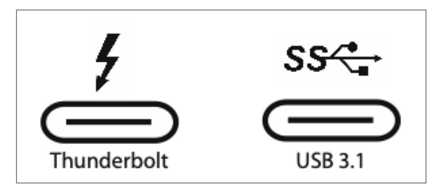


Abb. 10.14: Thunderbolt- und USB-Logos

Die Datenübertragungsrate von Thunderbolt ist enorm. Thunderbolt 1 überträgt im Vollduplexmodus 10 Gbps und ist mit dem derzeit schnellsten USB-Standard (3.1) vergleichbar. Thunderbolt 2 kombiniert die internen Datenkanäle und ermöglicht einen Datendurchsatz von bis zu 20 Gbps. Thunderbolt 3 verdoppelt diesen Wert noch einmal auf 40 Gbps, benötigt dabei aber nur halb so viel Energie wie Thunderbolt 2. Das nenn ich flott!

Wichtig

Für die CompTIA A+-Prüfungen sollten Ihnen Merkmale und Zweck von USB- und Thunderbolt-Schnittstellen geläufig sein.

10.1.5 Allgemeine Probleme mit Anschlüssen

Egal, welchen Anschlusstyp Sie auch verwenden, wenn er nicht funktioniert, sollten Sie immer ein paar Dinge prüfen. Als Erstes sollten Sie feststellen, ob es sich um ein Problem des Anschlusses oder des Geräts handelt. Am besten schließen Sie dazu ein bekanntermaßen funktionierendes Gerät an denselben Anschluss an, und prüfen, ob es dort funktioniert. Falls nicht, dann handelt es sich sehr wahrscheinlich um ein Problem des Anschlusses. Es ist auch nicht verkehrt, den umgekehrten Weg zu beschreiten und das suspekte Gerät mit einem Anschluss zu verbinden, von dem Sie wissen, dass er funktioniert.

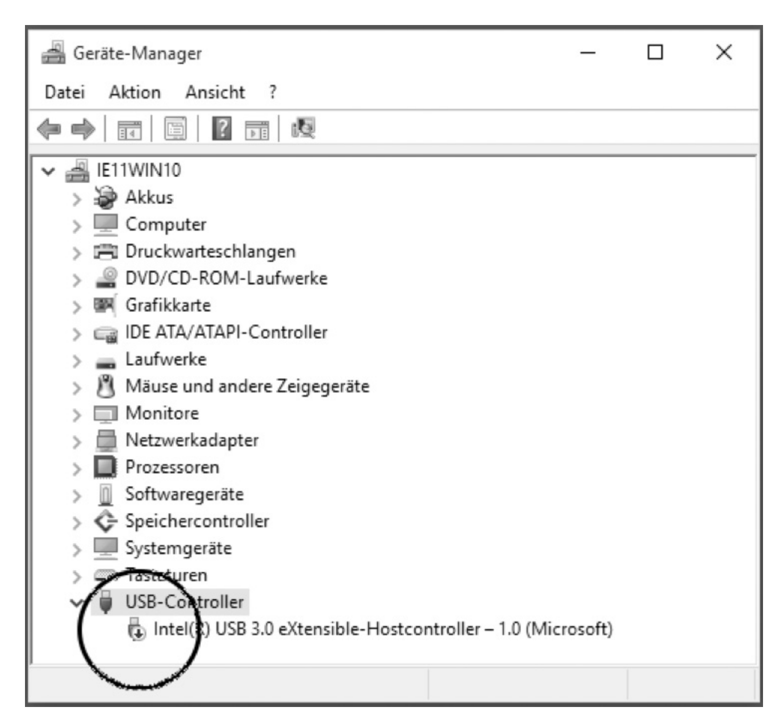


Abb. 10.15: Deaktivierter USB-Controller im Geräte-Manager von Windows 10

Wenn Sie sicher sind, dass der Anschluss nicht funktioniert, sollten Sie drei Dinge prüfen: Erstens sehen Sie nach, ob der Anschluss auch aktiviert ist. Nahezu alle E/A-Anschlüsse auf einem Mainboard lassen sich über das CMOS deaktivieren. Starten Sie das System neu, suchen Sie die Komponente und prüfen Sie, ob sie deaktiviert wurde. Über den Geräte-Manager von Windows lassen sich die meisten Komponenten und Anschlüsse ebenfalls deaktivieren. Abbildung 10.15 zeigt einen deaktivierten USB-

Controller im Geräte-Manager. Ein nach unten weisender Pfeil neben dem Symbol der Komponente zeigt an, dass diese deaktiviert wurde (oder nicht funktioniert). Um den Anschluss wieder zu aktivieren, klicken Sie das Symbol der Komponente mit der rechten Maustaste an und wählen im Kontextmenü AKTIVIEREN.

Anschlüsse brauchen Treiber, so wie Geräte Treiber brauchen. Da alle Betriebssysteme über ausgezeichnete integrierte Treiber für alle verbreiteten Anschlüsse verfügen, können Sie, wenn ein Anschluss im Geräte-Manager nicht angezeigt wird (und er im CMOS aktiviert ist), davon ausgehen, dass es sich um ein physisches Problem des Anschlusses handelt.

Tipp: Erweiterungsmöglichkeiten

Die Hersteller entwickeln kontinuierlich neue Erweiterungskarten und Peripheriegeräte, um ihren Kunden die neueste Technologie anbieten zu können. Überprüfen Sie, welche Anschlüsse in Ihrem System verfügbar sind. Was ist vorhanden? Suchen Sie anschließend im Internet nach Upgrades. Können Sie eine PCIe-USB-3.1-Karte mit Anschlüssen des Typs C verwenden? Wie sieht es mit einer zusätzlichen Thunderbolt-Karte aus? Oder suchen Sie nach aktiven oder passiven USB-Hubs. Welche Varianten sind erhältlich?

10.2 Standard-Ein-/Ausgabegeräte

Peripheriegeräte erweitern die Funktionalität des Computers. Dazu gehören natürlich Maus und Tastatur, aber es gibt noch viele weitere. In den CompTIA A+-Prüfungen werden viele andere Geräte als Standard-Ein-/Ausgabegeräte betrachtet. Hier die Liste für dieses Kapitel:

- Tastaturen
- Zeigegeräte
  - Mäuse
  - Touchpad
- Biometrische Geräte
- Smartcard-Lesegeräte
- Barcode-Lesegeräte
- Touchscreen-Bildschirme
- KVM-Umschalter
- Gamepads und Joysticks
- Grafiktabletts
- Multimediageräte
  - Digitalkameras
  - Webcams
  - Soundkarten, Lautsprecher und Mikrofone
- Viele dieser »Standard«-Geräte werden Sie im Alltag wohl kaum benutzen, daher sehen wir sie uns der Reihe nach etwas näher an. (Weiteren gängigen Peripheriegeräten, nämlich Videoaufzeichnungskarten, TV-Empfängern, Druckern und Scannern, ist ein eigenes Kapitel gewidmet.)

10.2.1 Tastaturen

Tastaturen stellen das älteste und immer noch das wichtigste Verfahren der Dateneingabe beim PC dar. Moderne Betriebssysteme enthalten für alle Tastaturen gut geeignete Treiber. Für einige Tastaturen mit Sonderfunktionen (Displays, Beleuchtung, programmierbare Tasten) werden jedoch spezielle Treiber benötigt, die installiert sein müssen, wenn die Geräte in vollem Umfang korrekt funktionieren sollen.

Moderne Tastaturen werden mit einem Kabel am USB-Anschluss angeschlossen oder sind drahtlos. In den letzten Jahren erlebte der alte, aber schnelle PS/2-Anschluss eine Renaissance. Abbildung 10.16 zeigt einen kombinierten Maus/Tastatur-Anschluss eines modernen Mainboards.



Abb. 10.16: PS/2-Anschluss für Maus/Tastatur (runder Anschluss oben links)

Hinweis

Wenn Sie eine drahtlose Tastatur verwenden, entfällt das Kabel von der Tastatur zum Computer. Stellen Sie aber sicher, dass stets Ersatzbatterien für die Tastatur verfügbar sind.

Bei einer Standardtastatur gibt es kaum etwas zu konfigurieren. Das einzige Konfigurationswerkzeug, das Sie möglicherweise benötigen, ist das Applet TASTATUR in der Systemsteuerung. Mit ihm können Sie die Verzögerung der Zeichenwiederholung (die Zeit, wie lange eine Taste gedrückt sein muss, bevor das Zeichen wiederholt wird), die Wiederholrate (wie schnell Zeichen nach Ablauf der Zeichenwiederholverzögerung wiederholt werden) und die Cursorblinkrate einstellen. Abbildung 10.17 zeigt das Standarddialogfeld EIGENSCHAFTEN VON TASTATUR von Windows, das von einigen Tastaturtreibern um zusätzliche Registerkarten erweitert wird.

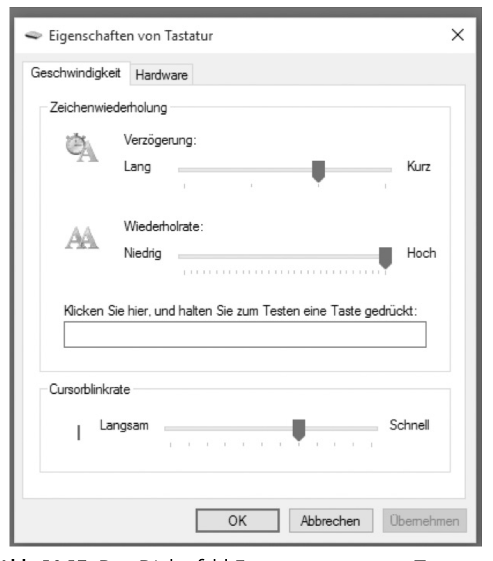


Abb. 10.17: Das Dialogfeld EIGENSCHAFTEN VON TASTATUR

Windows und Linux verwenden die gleichen QWERTZ-Tastaturen, inklusive der Sondertasten Strg und Alt, mit denen Sie Tastaturkürzel eingeben können. (Drücken Sie beispielsweise Strg + Z, um einen Vorgang rückgängig zu machen.) Für Windows ausgelegte Tastaturen besitzen eine Windows-Taste. Apple-Tastaturen verfügen (die Feststelltaste nicht mitgezählt) über drei Sondertasten: ctrl-Taste, Wahltaste ⌥ und Befehlstaste ⌘. Die ersten beiden sind die Pendants zu den Tasten Strg und Alt. Die Befehlstaste entspricht in etwa der Windows-Taste. Sie können eine Windows-Tastatur auch mit macOS verwenden, müssen aber die Systemeinstellung TASTATUR aufrufen, um die Belegung der Sondertasten anzupassen (Abbildung 10.18).



Abb. 10.18: Tastaturoptionen in den Systemeinstellungen von macOS

Tastaturen sind zwar einfach zu installieren, fallen aber manchmal aus. Abhängig von ihrem Standort – direkt vor Ihnen – verursachen drei Dinge die meisten Tastaturprobleme: verschüttete Flüssigkeiten, physische Beschädigungen und Schmutz.

Wenn Sie Limonade in Ihre Tastatur schütten, kann der Tag gelaufen sein. Falls Sie schnell sind und die Tastatur vom PC entfernen, bevor die Flüssigkeit die elektrischen Komponenten erreicht, können Sie die Tastatur möglicherweise noch retten. Sie muss jedoch gereinigt werden. Häufig haben Sie es dann aber mit einer klebrigen, schlecht funktionierenden Tastatur zu tun. Das sollten Sie sich wirklich nicht antun und sie besser austauschen!

Andere häufig auftretende physische Beschädigungen rühren von Dingen her, die auf die Tastatur fallen, wie beispielsweise einem schweren Buch (wie das in Ihren Händen). Das kann schlimme Folgen haben! Die meisten Tastaturen sind aber ziemlich robust und überleben meist auch den einen oder anderen Sturz vom Schreibtisch.

Entfernen Sie Schmutz und Ablagerungen auf den Tasten mit einem leicht mit Wasser befeuchteten Tuch. Wenn Wasser allein nicht ausreicht, können Sie auch ein bisschen Isopropanolalkohol auf das Tuch geben (Abbildung 10.19).

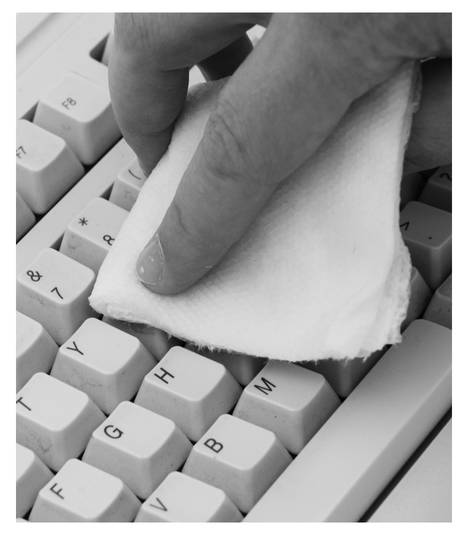


Abb. 10.19: Reinigung der Tasten

Schmutzige Tasten sehen lediglich unschön aus, Schmutz unter den Tasten kann aber dafür sorgen, dass die Tastatur überhaupt nicht mehr funktioniert. Wenn Tasten hängen bleiben, verwenden Sie eine Spraydose mit Druckluft, um sie zu reinigen. Machen Sie das am besten draußen oder über einem Mülleimer, denn es kann sich eine Menge Unrat unter den Tasten ansammeln.

Wenn einzelne verklebte Tasten völlig unbrauchbar geworden sind, ist letzten Endes die gesamte Tastatur nutzlos und Sie können versuchen, sie zu reinigen. Schlimmstenfalls müssen Sie sich dann eine neue kaufen.

10.2.2 Zeigegeräte

Haben Sie schon einmal versucht, ohne Maus mit Windows oder macOS zu arbeiten? Das macht zwar keinen Spaß, ist aber möglich. Alle Techniker lernen irgendwann die Navigationstasten von Windows kennen, für den Fall, dass Mäuse ausfallen, aber alles in allem lieben wir unsere Mäuse. Zum Bewegen des Mauszeigers sind zwei Geräte gebräuchlich, nämlich Mäuse und Touchpads. Wenn Sie die Maus bewegen, bewegt sich auch der Mauszeiger. Bei einem Touchpad streichen Sie mit dem Finger über dessen Oberfläche, um den Mauszeiger zu bewegen.

In macOS hat Apple die Messlatte für Touchpads mit Multi-Touch-Gesten etwas höher gelegt, auch für die in Apples Laptops verbauten und das Magic Trackpad. Wenn Sie beispielsweise mit zwei Fingern streichen, können Sie auf einer Seite hoch- oder runterscrollen. Oder wenn Sie einen Haufen Fenster geöffnet haben und auf den Schreibtisch zugreifen möchten, dann spreizen Sie einfach Ihren Daumen und drei Finger auf dem Touchpad auseinander. Haben Sie etwas Interessantes auf einer Webseite oder in einem PDF entdeckt? Tippen Sie zweimal mit zwei Fingern darauf, um es zu vergrößern. Erneutes doppeltes Tippen verkleinert es wieder. Die Liste möglicher Kombinationen ließe sich fortsetzen. Sie können sie unter `https://support.apple.com/de-de/HT204895` nachlesen.

In Windows werden die Einstellungen von Maus oder Touchpad über das Applet MAUS in der Systemsteuerung angepasst. Abbildung 10.20 zeigt die Version von Windows 7. In den Systemeinstellungen von macOS gibt es für Maus und Trackpad jeweils ein eigenes Applet.

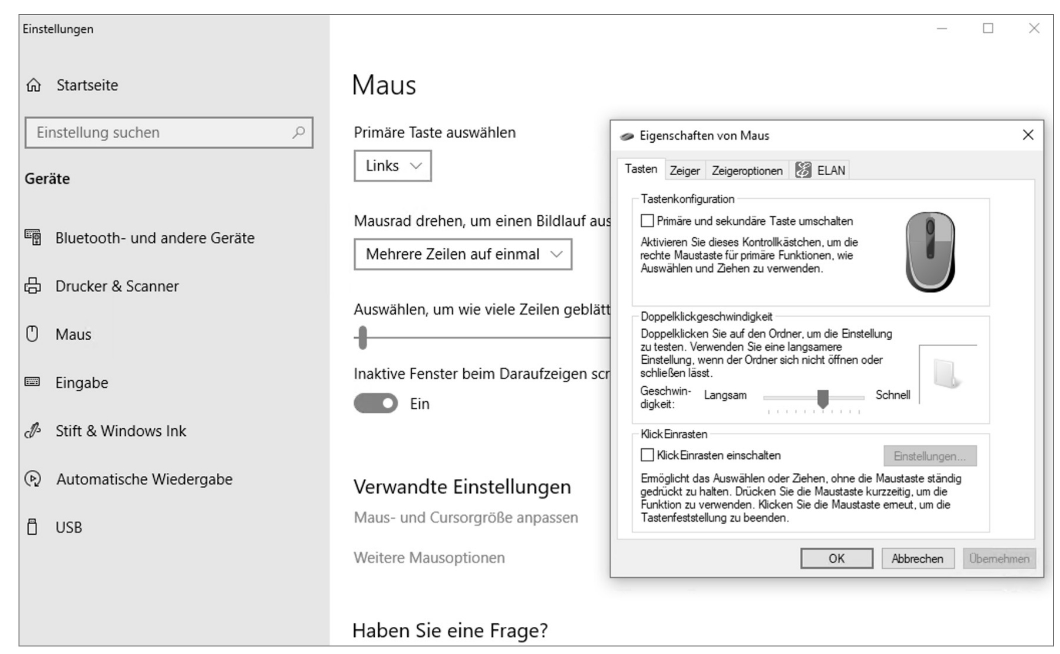


Abb. 10.20: Einstellungen der Maus und das Dialogfeld EIGENSCHAFTEN VON MAUS

Moderne Zeigegeräte benötigen nur wenig Wartungsaufwand und müssen fast nie gereinigt werden, weil ihre Optik nie in direkten Kontakt mit der rauen Außenwelt kommt. Sollte sich eine optische Maus dennoch einmal fehlerhaft verhalten, versuchen Sie, den Schmutz, der möglicherweise die Optik blockiert, mit einem feuchten Baumwolltuch zu entfernen (Abbildung 10.21).

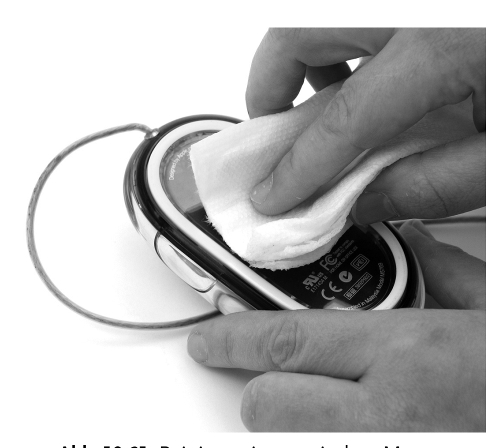


Abb. 10.21: Reinigen einer optischen Maus

10.2.3 Biometrische Geräte

Biometrische Geräte scannen bestimmte Körperteile (z.B. Netzhaut, Iris, Gesicht oder Fingerabdrücke) mit Abtastgeräten. Die Daten werden dann als elektronischer Schlüssel benutzt, um unberechtigte Personen daran zu hindern, auf geschützte Dinge zuzugreifen. macOS und Windows 10 bringen Unterstützung für biometrische Geräte wie Fingerabdruckscanner mit (Abbildung 10.22). Windows

verwendet Windows Hello zur Handhabung biometrischer Authentifizierung. In Abbildung 10.23 trainiere ich mein System mit einer zu Windows Hello kompatiblen Infrarotkamera darauf, mein Gesicht zu erkennen.



Abb. 10.22: Laptop mit integriertem Fingerabdruckscanner

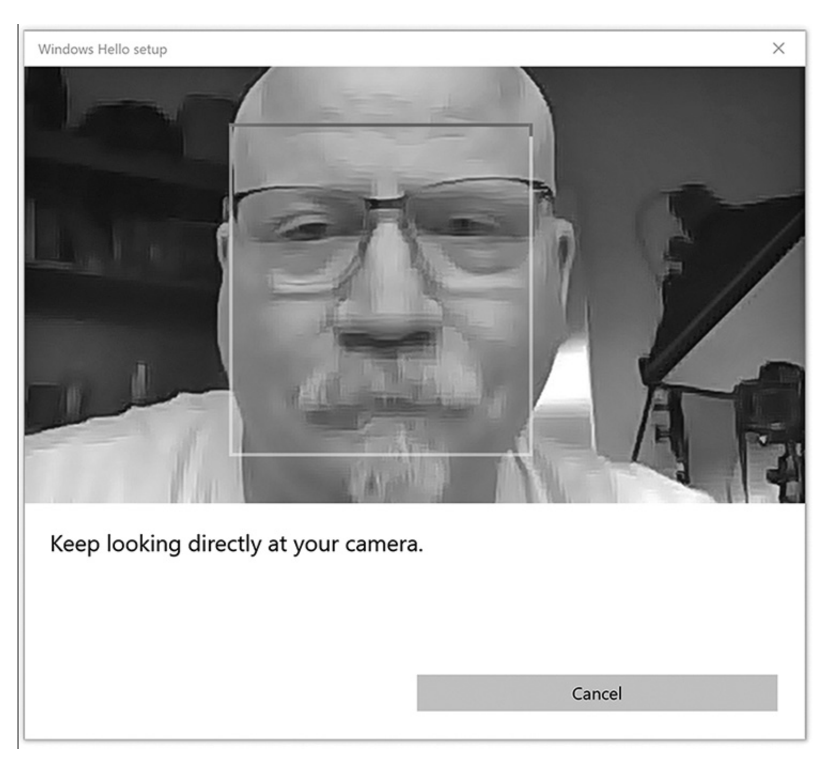


Abb. 10.23: Training der Gesichtserkennung

Biometrischer Schutz ist bei Smartphones sehr verbreitet. Sowohl Apple als auch andere Anbieter unterstützen Fingerabdruckscanner für Smartphones, die entsprechend ausgerüstet sind. Sie ersetzen den Schutz durch eine PIN oder ein Kennwort. Abbildung 10.24 zeigt, wie der Fingerabdruckscanner von Android einen neuen Fingerabdruck erlernt. Wenn Sie von Android oder einem Programm dazu

aufgefordert werden, legen Sie einfach Ihren Finger auf den Fingerabdruckscanner. Dadurch wird Ihre Identität bestätigt (sofern Ihr Fingerabdruck mit dem hinterlegten übereinstimmt), und spezielle Software, die zum Scanner gehört, übergibt Ihre Anmeldedaten an das System.

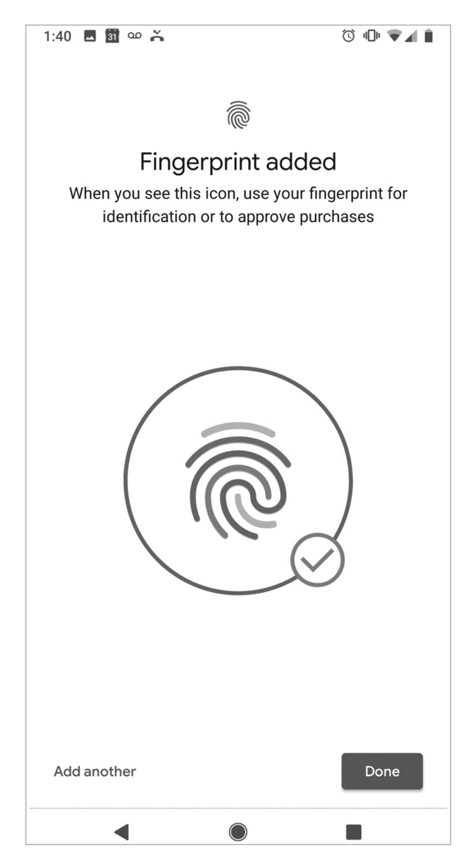


Abb. 10.24: Fingerabdruckscanner eines Android-Smartphones

Biometrische Geräte werden auch zu Erkennungszwecken verwendet. Erkennung unterscheidet sich dahin gehend von der Sicherheit, dass es hier dem biometrischen Gerät egal ist, wer Sie sind, denn es interessiert sich nur dafür, was Sie machen. Das beste Beispiel hierfür sind Spracherkennungsprogramme, die Spracheingaben in Befehle oder Text umwandeln. Apple, Microsoft und Google setzen Spracherkennung in vielfältiger Form ein, beispielsweise bei den charmanten Sprachassistentinnen Siri in iOS oder Cortana in Windows 10. Beide beantworten Anfragen und nehmen Anweisungen entgegen. Google verwendet in dem Aushängeschild für Büroanwendungen, Google Docs, ebenfalls Spracherkennung, sodass der Benutzer Eingaben nicht nur mit der Tastatur, sondern auch durch Sprache vornehmen kann.

Egal welche biometrischen Geräte Sie nutzen, die Einrichtung erfolgt immer auf dieselbe Weise:

1. Sie installieren das Gerät.
2. Sie registrieren sich bei dem Gerät, indem Sie ihm Ihr Auge, Ihren Finger, Ihr Gesicht etc. präsentieren.
3. Sie konfigurieren die zugehörige Software, um dem Gerät mitzuteilen, was es tun soll, wenn es Sie erkennt.

10.2.4 Smartcard-Lesegeräte

Viele Unternehmen nutzen Smartcards, um ihren Angestellten den Zugriff auf bestimmte Ressourcen oder den Zugang zu Räumlichkeiten zu ermöglichen. *Smartcard-Lesegeräte* gibt es in den verschiedensten Formen. So gibt es etwa kleine Geräte, die am Laptop angeschlossen werden (Abbildung 10.25), oder Bedienfelder zur Absicherung von Türen. Das Lesegerät scannt dabei einen Chip, der sich in einer Art Ausweiskarte befindet, um die Sicherheit zu erhöhen und Zugang zu gewähren.



Abb. 10.25: Smartcard-Lesegerät

10.2.5 Barcode- und QR-Lesegeräte

Barcode-Lesegeräte sollen standardisierte *UPC-Strichcodes* (*Universal Product Code*) oder QR-Codes (Quick-Response-Codes) einlesen (Abbildung 10.26). Das Einlesen der Barcodes ermöglicht beispielsweise die einfache elektronische Überwachung der eigenen Lagerbestände. Beim Einsatz von Barcode-Lesegeräten können die auf Rechnern gespeicherten Lagerbestände in den Datenbanken schnell und automatisch aktualisiert werden.



Abb. 10.26: UPC-Strichcode (links) und QR-Code (rechts)

Am PC begegnet man vor allem zwei Arten von Barcode-Lesegeräten, Stift- und Handscannern. *Stiftscanner* (Abbildung 10.27) sehen aus wie ein Schreibgerät, und der Benutzer muss damit über den Barcode streichen. *Handscanner* werden vor den UPC-Code gehalten, der beim Drücken eines Tasters eingelesen wird. Alle Barcode-Lesegeräte geben nach dem Scannen zur Bestätigung einen Ton aus, damit man weiß, dass der Code erfolgreich eingelesen wurde.



Abb. 10.27: Barcode-Handscanner

Barcode-Lesegeräte verwenden den USB-Anschluss oder funktionieren drahtlos. Normalerweise müssen sie nicht weiter konfiguriert werden, wenn man einmal davon absieht, dass das jeweilige Barcode-Lesegerät mit den für die Datenbank oder den Kassiervorgang verwendeten Programmen zusammenarbeiten muss.

10.2.6 Touchscreen-Bildschirme

Bei *Touchscreens* handelt es sich um Bildschirme, deren Oberfläche berührungsempfindlich ist und die Position und Dauer des Kontakts eines Fingers oder eines Stifts erkennen können. Alle Touchscreen-Bildschirme geben die Berührungsdaten so an den Rechner weiter, als ob es sich um Mausereignisse handeln würde. Touchscreens werden dann verwendet, wenn die traditionelle Maus- oder Tastatureingabe unmöglich oder ungeeignet ist. Hier einige Einsatzgebiete von Touchscreen-Bildschirmen:

- Smartphones
- Smartwatches
- Fitnessarmbänder
- Informationsstände
- Verkaufssysteme (POS-Terminals/Point-Of-Sale-Systeme)
- Tablet-PCs
- E-Book-Lesegeräte

Touchscreen-Bildschirme können in zwei Gruppen eingeordnet werden: eingebaute Bildschirme (z.B. bei Smartphones) und eigenständige Touchscreen-Bildschirme, wie man sie bei vielen Verkaufssystemen findet. Aus der Sicht des Technikers können Sie sich einen eigenständigen Touchscreen wie einen Bildschirm mit integrierter Maus vorstellen. Alle Touchscreens besitzen separate USB-Anschlüsse für ihre Mauskomponente, für die möglicherweise spezielle Treiber installiert werden müssen.

Windows enthält in der Systemsteuerung Applets zur Konfiguration des Touchscreens von Tablet-PCs wie dem Microsoft Surface. In Windows gibt es die Einstellung TABLET-MODUS für Computer mit berührungsempfindlichem Bildschirm, über den manche Laptops verfügen (Abbildung 10.28; beachten Sie, dass dieses Applet nur auf Tablet-PCs mit Touchscreen angezeigt wird, wie beispielsweise auf einem Microsoft Surface.) Sie können damit, ähnlich wie in den Applets MAUS und TASTATUR, anpassen, auf welche Weise Sie mit dem berührungsempfindlichen Bildschirm interagieren. So können Sie etwa festlegen, was beim Antippen, doppeltem Antippen oder anderen Fingergesten geschehen soll.

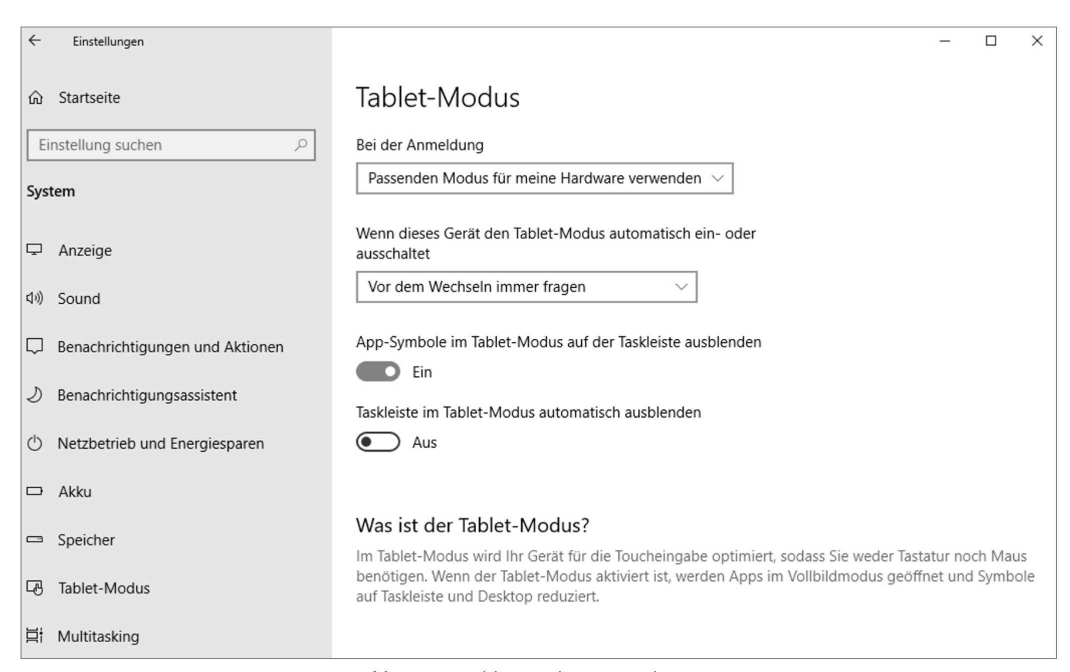


Abb. 10.28: Tablet-Modus in Windows 10

10.2.7 KVM-Umschalter

Ein *KVM-Umschalter* (Keyboard, Video, Mouse) ist ein Gerät, das zumeist dafür sorgt, dass mehrere Rechner über eine einzige Maus, eine einzige Tastatur und einen einzigen Bildschirm bedient werden können. Bei einigen KVMs wird diese Funktion umgekehrt, sodass einzelne Rechner über mehrere Tastaturen, Mäuse oder andere Geräte bedient werden können. KVMs sind insbesondere nützlich, wenn in einem Datencenter mehrere Rechner in Serverschränken montiert sind, der Platz beschränkt und der Energieverbrauch von Bedeutung ist. Ein Administrator kann dann über einen KVM-Umschalter mehrere Serversysteme über eine Tastatur, eine Maus und einen Bildschirm bedienen.

Es gibt eine Menge verschiedener KVM-Umschalter. An manche lassen sich nur zwei Systeme anschließen und andere steuern Hunderte. Einige besitzen zusätzlich Audiobuchsen zum Anschluss von Lautsprechern. Typischen KVM-Umschaltern liegen zwei oder mehr Kabelsätze bei, mittels derer die Eingabegeräte (PS/2- oder USB-Anschluss für Maus und Tastatur) und die Bildschirmausgänge der Rechner mit dem Umschalter verbunden werden (Abbildung 10.29).

Um einen KVM-Umschalter zu verwenden, schließen Sie einfach eine Tastatur, eine Maus und einen Bildschirm an den Umschalter an und verbinden dann die Rechneranschlüsse mit den entsprechenden KVM-Anschlüssen. Wenn die Anschlüsse korrekt verbunden sind und der Umschalter richtig konfiguriert ist, können Sie mit bestimmten Tastenkombinationen, die vom KVM-Hersteller vorgegeben werden, zwischen den an den Umschalter angeschlossenen Rechnern hin- und herwechseln. Zum Umschalten zwischen den Sitzungen wird oft die zweifache Betätigung der Taste `Rollen` verwendet.

Die Installation eines KVM-Umschalters ist nicht schwierig. Sie müssen dabei lediglich darauf achten, dass Sie die Rechner einzeln und nacheinander mit den Kabelsätzen an den Umschalter anschließen, damit nicht versehentlich die Maus den einen und die Tastatur einen anderen Rechner bedient, während die Bildschirmausgabe von wieder einem anderen Computer stammt. (Ich kann Ihnen nur dringend empfehlen, die Kabel mit Aufklebern zu kennzeichnen und Kabelbinder zu benutzen.)



Abb. 10.29: Ein typischer KVM-Umschalter

Wenn mit den Anschlüssen etwas nicht stimmt, dann funktioniert der KVM-Umschalter nicht wie gewünscht. Das Ergebnis habe ich eben bereits beschrieben. Verwechseln Sie also nicht die Kabelanschlüsse!

10.2.8 Gamepads und Joysticks

Wenn Sie mit Höchstgeschwindigkeit durch eine enge Kurve rasen oder einen nagelneuen Düsenjet fliegen, ist es für ein großartiges Spielerlebnis durchaus von Bedeutung, die richtige Steuerung dafür zu verwenden. Dazu werden üblicherweise Gamepads und Joysticks eingesetzt.

Insbesondere PC-Spiele, die eigentlich für Spielkonsolen wie die Xbox One von Microsoft oder die Playstation 4 von Sony ausgelegt sind, lassen sich am besten mit einem *Gamepad* steuern. Ein Gamepad ähnelt eher einer normalen Videospielsteuerung und ist üblicherweise mit einer Reihe von Knöpfen und Schaltern übersät, die Bewegungen und Aktionen auf dem Bildschirm auslösen (Abbildung 10.30).



Abb. 10.30: Ein Gamepad

In den letzten zehn Jahren haben Flugsimulatoren an Beliebtheit verloren und dementsprechend auch *Joysticks* (Abbildung 10.31). Joysticks gehörten früher zur Standardausrüstung eines jeden Spielers, werden heute aber nur noch von *ernsthaften* Flugsimulator-Fans benötigt. Die meisten modernen Spiele werden entweder per Gamepad oder via Maus und Tastatur gesteuert.



Abb. 10.31: Ein Joystick

Joysticks und Gamepads haben im Laufe der Jahre viele verschiedene Anschlüsse verwendet, darunter natürlich auch den namensgebenden Joystick-Anschluss. Heutzutage werden sie entweder per USB angeschlossen oder arbeiten drahtlos. Je nach Funktionsumfang kann es erforderlich sein, dass Treiber installiert werden müssen, damit das Steuergerät funktioniert.

Damit alle Knöpfe und Schalter wunschgemäß funktionieren, müssen Sie Ihren Joystick oder Ihr Gamepad konfigurieren. Sie müssen dazu in Windows im Startmenü GERÄTE UND DRUCKER öffnen und dann mit der rechten Maustaste auf Ihr Steuergerät klicken und GAMECONTROLLEREINSTELLUNGEN auswählen. Wählen Sie Ihr Modell aus der Liste der Controller aus und klicken Sie auf EIGENSCHAFTEN. Nun können Sie, je nach verwendetem Joystick oder Gamepad, die verschiedenen Knöpfe, Schalter usw. Ihren Wünschen entsprechend konfigurieren (Abbildung 10.32). Hier können Sie beispielsweise die analogen Steuerknüppel kalibrieren, damit diese Ihre Aktionen korrekt widerspiegeln. Außerdem wird hier die Stärke der Vibrationen beim *Force Feedback* geregelt (falls bei Ihrem Gerät verfügbar).

Hinweis

Unter Umständen müssen Sie auch innerhalb des Spiels, das Sie steuern möchten, Einstellungen vornehmen. Die meisten Spiele sind so voreingestellt, dass die Steuerung mittels Maus und Tastatur erfolgt. Probieren Sie einfach aus, welche Einstellung für Ihr Gerät erforderlich ist.

Sobald Sie Ihr Steuergerät eingerichtet haben, steht Ihnen der Himmel offen und die Straße ist frei!

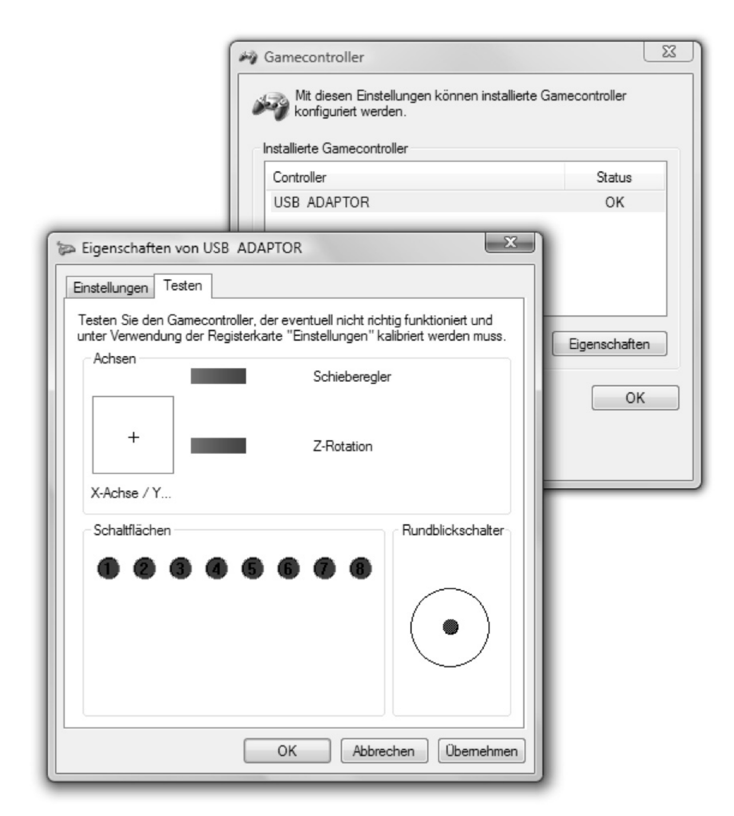


Abb. 10.32: EIGENSCHAFTEN-Dialogfeld eines Gamecontrollers

10.2.9 Grafiktabletts

PCs und Macs sind für bildende Künstler schnell zum leistungsfähigsten und flexibelsten Werkzeug geworden. Angesichts der Vielzahl von Software, die sich dem Erstellen von Grafiken und Bildern auf unterschiedlichste Weise (wie Malen, Zeichnen, Animieren usw.) widmen, steht die digital erstellte Kunst auf einer Stufe mit ihrem traditionellen Pendant. Es ist daher nur vernünftig, dass entsprechende Geräte entwickelt wurden, die es den Benutzern erlauben, von all dieser Software zu profitieren.

Ein Grafiktablett erlaubt es dem Benutzer, am Computer zu malen, zu zeichnen oder mit der Hand zu schreiben (Abbildung 10.33). Fangen Sie nun aber nicht damit an, mit Aquarellfarben auf Ihrem Bildschirm herumzupinseln. Das Grafiktablett nimmt Eingaben mittels einer speziellen Oberfläche entgegen. Wenn der Benutzer diese Oberfläche (normalerweise mit einem Stift) berührt, werden dessen Bewegungen in digitale Informationen transformiert (oder digitalisiert). Das Zeichen- oder Malprogramm empfängt diese Informationen und stellt sie in Form eines Bildes auf dem Bildschirm dar (Abbildung 10.34). Wenn Sie beispielsweise auf dem Grafiktablett eine Linie zeichnen, sollte diese auch auf dem Bildschirm erscheinen.

Hinweis

Nicht alle Grafiktabletts sind zum Malen oder Zeichnen gedacht. Es gibt auch Modelle, die für Handschrifterkennung, technische Zeichnungen, den Entwurf komplexer Buchstaben oder sogar als Mausersatz verwendet werden.



Abb. 10.33: Ein Wacom-Grafiktablett

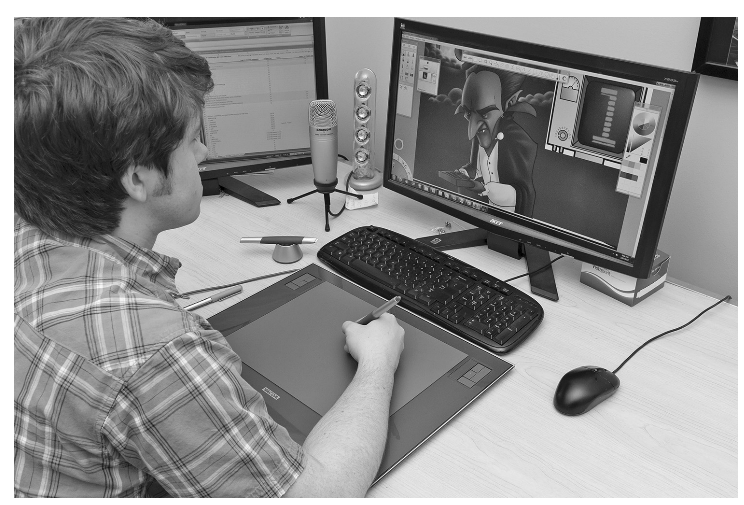


Abb. 10.34: Zeichnen mit einem Grafiktablett

Die meisten Grafiktabletts werden über USB am Computer angeschlossen oder arbeiten drahtlos. Vorher müssen Sie Treiber installieren, die aber normalerweise mitgeliefert werden. Es gibt für gewöhnlich außerdem eine Software zur Konfiguration, mit der die Druckempfindlichkeit des Tabletts, die Belegung von Tasten des Tabletts und der Bildschirmbereich, auf dem mit dem Grafiktablett gezeichnet werden kann, einstellbar sind.

Viele Leute interagieren mit einer sehr einfachen Digitalisierungstechnologie, wenn sie den Empfang von Paketen quittieren. Sie unterzeichnen auf einem kleinen Gerät, nicht selten ein Smartphone, das die Unterschrift digitalisiert.

10.2.10 Multimediageräte

Viele Leute verwenden Multimediageräte wie Digitalkameras und Webcams, um Fotos zu teilen und sich per Videochat mit Freunden und Verwandten rund um den Globus zu unterhalten. Und schließ-

lich bieten fast alle Geräte irgendeine Möglichkeit, Sprache und Musik aufzuzeichnen und wiederzugeben.

Digitalkameras

Digitalkameras sind unverzichtbare Werkzeuge, um Momentaufnahmen festzuhalten und diese Freunden und Verwandten zuzusenden. Da offenbar in fast allen technischen Geräten mittlerweile eine Digitalkamera verbaut ist, möchte ich klarstellen, dass es hier um *richtige* Kameras geht, die zum Erstellen hochwertiger Fotos gedacht sind. Weil diese Digitalkameras an Computer angeschlossen werden können, sollten CompTIA A+-zertifizierte Techniker ihre Grundlagen kennen.

Speichermedien Digitalkameras und Camcorder speichern die mit ihnen aufgenommenen Bilder und Videos auf irgendwelchen Wechseldatenträgern. Der vermutlich gebräuchlichste Wechseldatenträger für moderne Digitalkameras ist die SD-Karte (Secure Digital) (Abbildung 10.35), es gibt aber weitere Typen, die Ihnen insbesondere bei Profi-Kameras begegnen. (Weitere Information zu Wechseldatenträgern finden Sie im Abschnitt 10.3, *Speichergeräte*, weiter hinten in diesem Kapitel.)



Abb. 10.35: Eine SD-Karte

Anschluss Fast alle modernen Digitalkameras lassen sich heute direkt mit einem USB-Anschluss oder über ein WLAN verbinden (Abbildung 10.36). Häufig wird auch nur das Speichermedium an den Computer angeschlossen, wozu digitale Kartenleser oder USB-Adapter verwendet werden können.

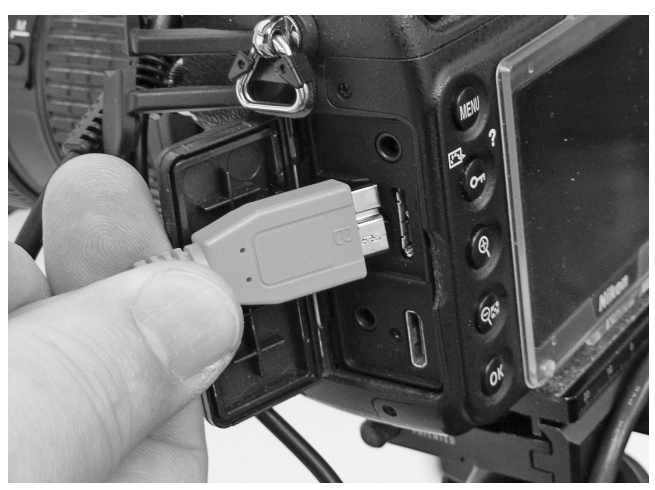


Abb. 10.36: USB-Anschluss einer Kamera

Es gibt Lesegeräte speziell für SD-Karten, aber auch andere Typen. Die meisten Lesegeräte können mehrere Datenträgerformate lesen. Viele Computer besitzen bereits eingebaute Mehrfach-Kartenleser (Abbildung 10.37).



Abb. 10.37: In einen Computer eingebauter Mehrfach-Kartenleser

Webcams

In einem Computer integrierte oder an einem Monitor befestigte Kameras werden meist als *Webcams* bezeichnet, weil sie bevorzugt für die Videokommunikation im Internet verwendet werden. Qualität und Preis von Webcams sind von großer Bandbreite.

Sowohl die Bild- als auch die Tonqualität von Webcams sind sehr unterschiedlich. Weil Webcams hauptsächlich für Videochats verwendet werden, bewerben die Hersteller sie oft wie andere Kameras mit Begriffen wie 720p, HD oder 4K. Die heutzutage verbreitetsten eigenständigen Webcams liefern eine Auflösung von 1080p HD, die in Laptops integrierten hingegen meist 720p.

Hinweis

Sind Ihnen Begriffe wie 1080p oder Pixel nicht geläufig? Lesen Sie in Kapitel 17 nach.

Abbildung 10.38 zeigt zwei meiner Redakteure beim Chatten per Webcam mit Skype.

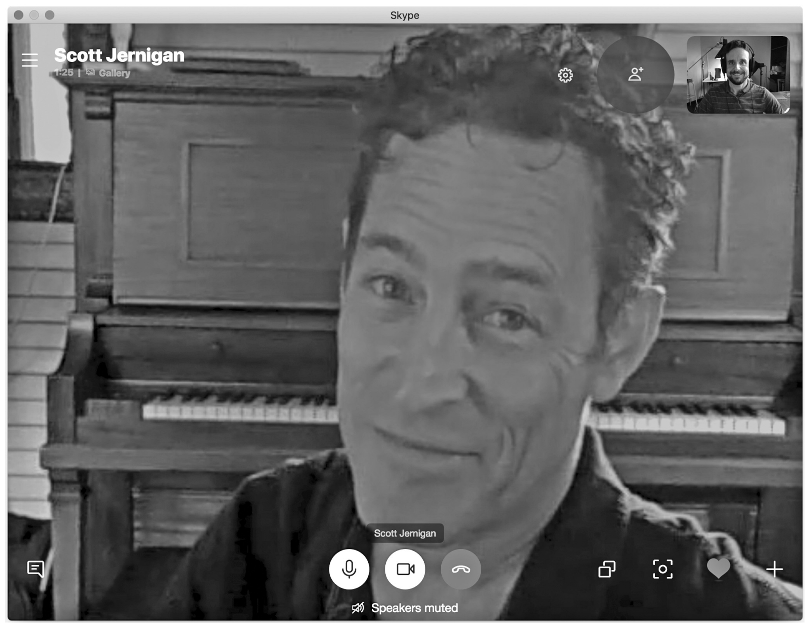


Abb. 10.38: Videounterhaltung per Webcam mit Skype

Die meisten Leute, die Online-Video nutzen, wünschen sich auch ein Mikrofon. Viele Webcams enthalten ein eingebautes Mikrofon, Sie können aber auch ein eigenständiges verwenden. Diejenigen unter Ihnen, die sehr viele Videounterhaltungen führen, bevorzugen möglicherweise eine Kamera ohne Mikrofon und kaufen sich ein qualitativ hochwertiges Headset, über das sie sprechen und hören können.

Soundkomponenten

Praktisch alle computerartigen Geräte sind heute mit den vier grundlegenden Komponenten ausgestattet, die für Aufzeichnung und Wiedergabe von Audiodaten benötigt werden: auf dem Mainboard integrierte Komponenten zur Tonerzeugung oder eine eigene Soundkarte, Lautsprecher, Mikrofon sowie Software zur Aufnahme und Wiedergabe von Audiodaten.

Analoger und digitaler Sound Die Aufzeichnung von Schallwellen erfolgt durch einen Prozess, der *Abtasten* bzw. *Sampling* genannt wird. Im einfachsten Sinne bedeutet Sampling die Aufzeichnung des Zustands oder der Eigenschaften einer bestimmten Schallwelle in einer bestimmten Häufigkeit je Sekunde. Die *Abtastrate* oder *Sampling-Rate* wird in Tausenden von Schwingungen je Sekunde bzw. Kilohertz (kHz) angegeben. Je häufiger eine Schallwelle abgetastet wird, desto naturgetreuer lässt sich der aufgezeichnete Ton reproduzieren. Die meisten Aufzeichnungen im PC-Bereich erfolgen mit Frequenzen zwischen 11 kHz (sehr niedrige Qualität, wie bei einem alten Telefon) und 192 kHz (äußerst hohe Qualität, besser als das menschliche Ohr).

Hinweis

Moderne Mainboards besitzen ausnahmslos integrierte Komponenten zur Tonerzeugung. Dennoch verwenden die meisten Techniker weiterhin den Begriff *Soundkarte*, selbst wenn es keine Erweiterungskarte zur Tonerzeugung gibt. Eigene Soundkarten werden für spezielle Aufgaben verwendet, etwa wenn der Computer in einem Tonstudio zum Einsatz kommt. Für typische Anwendungen ist der eingebaute Sound für die meisten Benutzer ausreichend.

Töne unterscheiden sich hinsichtlich ihrer Lautstärke (*Amplitude*), ihrer Tonhöhe (*Frequenz*) und den Eigenschaften, die Noten voneinander unterscheiden, wenn sie auf verschiedenen Instrumenten gespielt werden (*Klangfarbe*). Alle Eigenschaften der jeweiligen Schallwelle (Amplitude, Tonhöhe und Klangfarbe) müssen aufgezeichnet und in Nullen und Einsen umgewandelt werden, um den Ton per Computer und über die Lautsprecher reproduzieren zu können.

Die Anzahl der Merkmalsausprägungen (unterschiedliche Signalpegel), die beim Abtasten eines bestimmten Tons aufgezeichnet werden können, werden über die *Abtasttiefe* (*Bittiefe* oder auch *Bitauflösung*) angegeben. Je höher die bei der Aufzeichnung eines Tons verwendete Abtasttiefe, desto mehr Merkmale lassen sich speichern und damit auch reproduzieren. Bei einem 8-Bit-Sample eines Gitarrensolos von Jimi Hendrix können z.B. nur $2^8 = 256$ verschiedene Signalpegel des Tons aufgezeichnet werden. Das würde sich wie eine billige Kopie einer Aufnahme anhören und klänge wahrscheinlich recht flau und dünn. Mit 16-Bit-Samples lassen sich hingegen $2^{16} = 65.536$ verschiedene Merkmalsausprägungen erfassen. Mit 16-Bit-Samples lassen sich alle vagen Obertöne und Rückkopplungen reproduzieren, die zu Hendrix' unverwechselbarem Sound beigetragen haben.

Der letzte Aspekt der Audioaufzeichnung betrifft die Anzahl der Spuren, die getrennt aufgenommen werden können. Meist zeichnet man nur eine einzelne Spur (*Mono*) oder zwei Spuren auf (*Stereo*). Spezielle Soundkarten lassen auch die gleichzeitige Aufzeichnung von mehr als zwei Tonspuren zu, aber dieses Thema würde den Rahmen des Buches sprengen.

Abtastrate und Bittiefe bestimmen gemeinsam, wie naturgetreu die Töne, die Sie hören, in ihre digitale Version überführt bzw. aufgezeichnet werden. Bei der Tonaufzeichnung spricht man von CD-Qualität, wenn diese mit einer Abtastrate von 44,1 kHz und 16 Bit Abtasttiefe in Stereo aufgenommen werden. Bei den meisten Aufnahmeprogrammen können Sie diese Werte vor der eigentlichen Aufnahme einstellen. Abbildung 10.39 zeigt die entsprechenden Einstellungen für Audacity, einem kostenlosen und leistungsfähigen Werkzeug zum Aufnehmen und Bearbeiten von Sound.

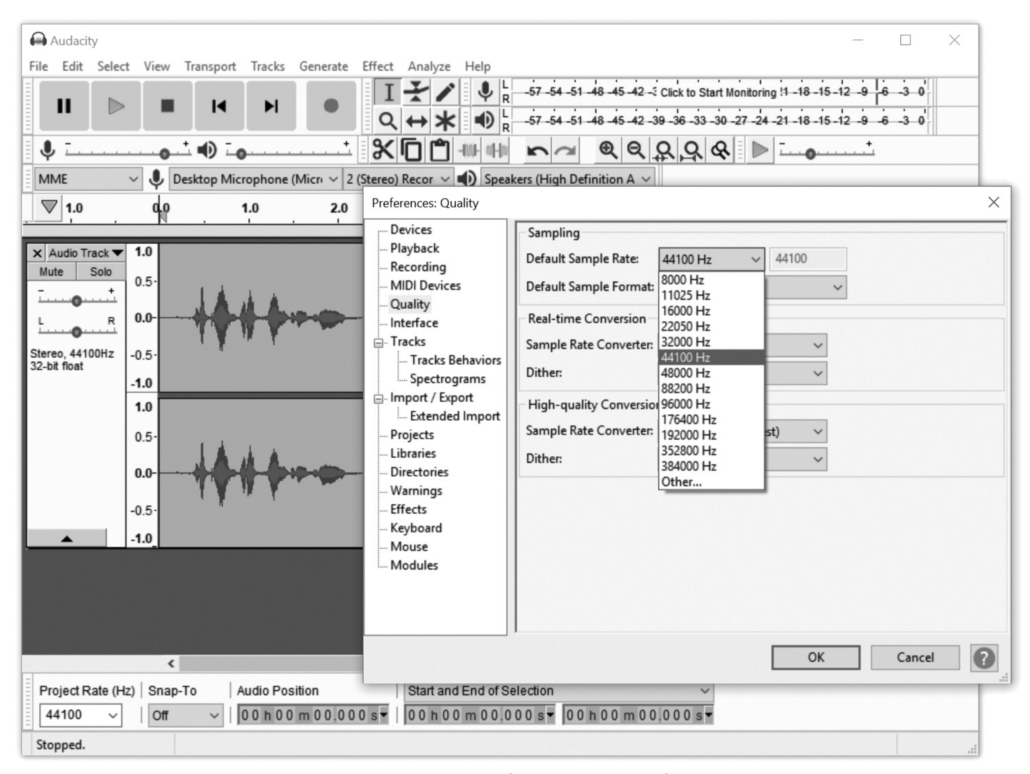


Abb. 10.39: Einstellung der Aufnahmeeigenschaften in Audacity

Sounddateiformate Für Audiodateien gibt es viele verschiedene Formate. *PCM* (*Pulse Code Modulation*) ist der Urahn aller Soundformate. PCM wurde in den Sechzigern zur Übertragung von Telefonanrufen über die ersten digitalen Leitungen entwickelt. Mit einigen wenigen Änderungen, die den Einsatz im PC-Bereich ermöglichen, wird das PCM-Format bis heute verwendet, auch wenn es hier meist mit dem verbreiteten *WAV*-Dateiformat gleichgesetzt wird. WAV-Dateien eignen sich zwar hervorragend zur naturgetreuen Aufzeichnung von Audiodaten, haben aber auch Nachteile. WAV-Dateien können ziemlich groß werden, insbesondere wenn sie mit hoher Abtastrate und hoher Bittiefe aufgezeichnet werden. Ein mit 44 kHz bei 16 Bit aufgezeichneter 4-Minuten-Song belegt z.B. schon mehr als 40 MB!

Interessant an der Aufnahmequalität ist, dass die Fähigkeiten des menschlichen Ohrs nicht ausreichen, um alle feinen Variationen unterschieden zu können, die in 16-Bit-Stereo/44,1-kHz-Dateien aufgezeichnet werden können. Clevere Programmierer haben Algorithmen geschrieben, mit denen Audiodaten komprimiert werden können. Diese Algorithmen – tatsächlich nur eine Reihe von Anweisungen als Code – werden als *Codecs* (Compressor/Decompressor) bezeichnet. Der vom Fraunhofer-Institut entwickelte MPEG-1-Layer-3-Codec ist der wohl bekannteste Codec. Wenn von ihm die Rede ist, dann meist nur mit der Dateinamenerweiterung der entsprechend codierten Audiodaten, nämlich *MP3*. Heutzutage ist das gebräuchlichste Format AAC (*Adanced Audio Encoding*), das von YouTube, iPhone und iPad und anderen verwendet wird.

Bei *Streaming* von Medien werden Daten übertragen, sofort wiedergegeben und anschließend gleich wieder verworfen bzw. gelöscht. Streaming ist im Internet unglaublich beliebt und hat mit den Internetradiosendern und Musikportalen eine ganze Industrie hervorgebracht.

MIDI Alle Soundkarten (integrierte und eigenständige) können auch selbst Töne erzeugen und nicht nur aufgezeichnete Audiodateien wiedergeben. Alle Soundkarten enthalten einen zweiten Prozessor,

der im *MIDI-Format* (*Musical Instrument Digital Interface*) gespeicherte Dateien interpretieren kann. Angemerkt werden muss, dass es sich, anders als bei einer WAV-Datei, bei einer MIDI-Datei nicht um eine eigenständige Audiodatei handelt. Während sich WAV-Dateien unabhängig von dem zur Wiedergabe verwendeten PC immer weitgehend gleich anhören, handelt es sich bei einer MIDI-Datei um eine Textdatei, die Anweisungen für vorhandene Audiohardware zur Erzeugung von Tönen enthält. Programmierer nutzen diese kleinen Dateien, um der Soundkarte mitzuteilen, welche Noten wie lange wie laut auf welchem Instrument gespielt werden sollen. Stellen Sie sich eine MIDI-Datei als ein elektronisches Notenblatt für die Soundkarte vor, wobei die Instrumente in die Soundkarte eingebaut sind.

Hinweis

Für MIDI-Dateien wird üblicherweise die Dateinamenerweiterung `.MID` verwendet. Sie stammt noch aus den Tagen von Microsofts erstem Betriebssystem DOS, bei dem Dateinamenerweiterungen auf drei Zeichen beschränkt waren.

Der besondere Vorteil von MIDI-Dateien besteht darin, dass sie – verglichen mit WAV-Dateien – winzig sind. Der erste Satz der fünften Symphonie von Beethoven belegt als hochwertige WAV-Datei z.B. satte 78 MB. Für dieselben ca. sieben Minuten werden in einer MIDI-Datei hingegen nur schlanke 60 KB benötigt. MIDI ist hardwareabhängig, daher entscheiden die Fähigkeiten und die Qualität der jeweiligen Soundkarte darüber, wie sich der reproduzierte Musiktitel anhört, wobei es haushohe Qualitätsunterschiede gibt.

Lautsprecherunterstützung Sie werden heutzutage Schwierigkeiten haben, ein Mainboard zu finden, das keine integrierte Soundkarte besitzt (Abbildung 10.40). Alle Mainboards unterstützen mindestens zwei Lautsprecher oder einen Stereokopfhörer, während viele Mainboards fünf oder mehr getrennte Lautsprecherkanäle unterstützen. Mit mehreren Lautsprechern lässt sich echter Surround-Sound erzeugen, der nicht nur bei Spielen, sondern auch bei der Filmwiedergabe über den PC häufig geschätzt wird. Das Mainboard in Abbildung 10.40 unterstützt beispielsweise mehrere Lautsprecher.

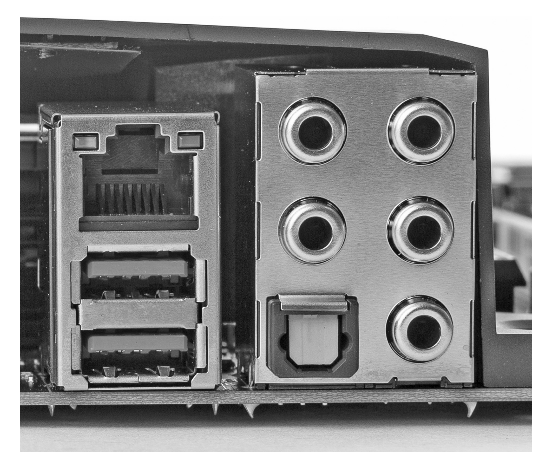


Abb. 10.40: Ein Mainboard mit mehreren Lautsprecheranschlüssen

Eine weitere beliebte Erweiterung von Lautsprechersystemen stellen *Subwoofer* dar. Subwoofer sind Basslautsprecher (*Tieftöner*), die für die beeindruckenden tieffrequenten Töne sorgen, die Ihren Filmen, Ihren Spielen und Ihrer Musik eine zusätzliche Klangdimension verleihen. Heutzutage unterstützen fast alle Soundkarten sowohl Surround-Sound als auch einen Subwoofer. In den Anzeigen müssen Sie hier auf Angaben wie *Dolby Digital* und *DTS* achten. Die Namensgebung für Lautsprechersysteme folgt einem einfachen System: ein 2.1-System besteht aus zwei Satelliten und einem Subwoofer (Abbildung 10.41). Ein 5.1-System besteht aus fünf Satelliten und einem Subwoofer.



Abb. 10.41: 2.1-Surround-Lautsprechersystem

Anschlussbuchsen Praktisch alle Soundkarten verfügen über mindestens drei Anschlüsse: einen für ein Stereolautsprechersystem mit integriertem Verstärker (*Line-Out*), einen für ein Mikrofon und einen Eingang, der *Line-In* genannt wird. Wenn Sie einen Blick auf die Rückseite eines Mainboards mit integrierter Soundkarte werfen, dann finden Sie dort unweigerlich diese drei Anschlüsse. Bei den meisten Systemen sind diese Anschlüsse farblich gekennzeichnet (Line-Out – Grün, Mikrofon – Pink, Line-In – Blau). Häufig finden Sie darüber hinaus noch weitere Anschlüsse (siehe Abbildung 10.40).

Sehen wir uns also an, wozu diese Anschlüsse dienen:

- **Main-Speaker Out**: Hierbei handelt es sich um den Haupt-Lautsprecherausgang, an den Sie Standardlautsprecher anschließen.
- **Line-Out**: Manche Soundkarten besitzen einen separaten Line-Out-Ausgang, der oft dazu verwendet wird, andere externe Aufnahmegeräte an den Rechner anzuschließen. Sie können über diesen Anschluss vom Computer erzeugte Sounds ausgeben.
- **Line-In**: An den Line-In-Eingang lassen sich z.B. CD- oder MP3-Player anschließen, um Audio mit dem Computer aufzunehmen.
- **Rear-Out**: Dieser Ausgang dient dem Anschluss der hinteren Lautsprecher eines Surround-Sound-Lautsprechersystems.
- **Analog/Digital Out**: Der multifunktionale Analog/Digital-out-Anschluss dient als spezielle digitale Verbindung zu externen digitalen Geräten oder digitalen Lautsprechersystemen und kann auch als analoger Anschluss für den mittleren Kanal vorn und den Subwoofer dienen.
- **Mikrofon**: An diesem Anschluss lässt sich ein externes Mikrofon zur Sprachaufzeichnung anschließen.

Viele Soundkarten verfügen zudem über einen speziellen S/PDIF-Anschluss (*Sony/Philips Digital Interface*), über den Sie die Soundkarte direkt mit einem 5.1-Lautsprechersystem oder einem entsprechenden Receiver verbinden können (Abbildung 10.42).

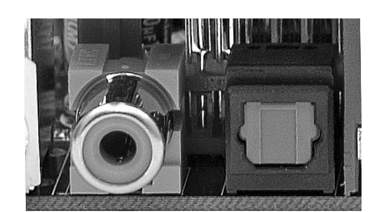


Abb. 10.42: S/PDIF-Anschlüsse

Wenn man einen einzigen S/PDIF-Ausgang anstelle separater Leitungen für die einzelnen Lautsprecher verwendet, vereinfacht das die Aufstellung der Lautsprecher deutlich. S/PDIF-Anschlüsse gibt es in zwei Varianten, optisch und koaxial. Die optische Variante sieht aus wie ein Quadrat mit einer kleinen Tür (in Abbildung 10.42 rechts). Beim Koaxial-Anschluss handelt es sich um einen normalen RCA-Anschluss (links), wie er auch zum Anschließen des CD-Players an die Stereoanlage verwendet wird. Es spielt keine Rolle, welche Anschlussvariante Sie verwenden, Sie müssen nur dafür sorgen, dass es einen freien Anschluss am Receiver oder den Lautsprechern gibt.

Hinweis

Sowohl HDMI als auch DisplayPort können Audio an einen Fernseher oder Receiver übertragen. Das ist praktisch, weil Sie nur ein Kabel für Audio und Video benötigen, wodurch alles aufgeräumter ist. Wenn Sie eine Karte verwenden, die Audio über HDMI/DisplayPort ausgeben kann, wird sie zusammen mit den normalen Lautsprechern und S/PDIF-Anschlüssen in den Einstellungen (Windows 10) und im Dialogfeld SOUND (alle Windows-Versionen) als Wiedergabegerät aufgeführt.

Unter Windows können Sie die Lautsprecher in der Systemsteuerung mit dem Applet SOUND konfigurieren. Die entsprechende Systemeinstellung in macOS heißt TON.

Mikrofone

Sie haben nun sicher keine Schwierigkeiten, geeignete Lautsprecher für die Wiedergabe von Musik zu finden. Aber was macht ein Musiker, der die eigene Musik aufnehmen möchte? Man benötigt natürlich ein *Mikrofon* zum Anschluss an die Soundkarte (Abbildung 10.43). Ein Mikrofon wandelt Schallwellen in elektrische Signale um und kann dadurch Töne aufzeichnen. Mikrofone werden vornehmlich zur Aufnahme von Stimmen verwendet, obwohl Sie selbstverständlich auch andere Klänge aufnehmen können.



Abb. 10.43: Ein typisches Mikrofon

Hinweis

Es gibt auch Mikrofone, die nicht an der Soundkarte, sondern per USB angeschlossen werden.

Headsets Falls Sie Musik hören möchten, ohne andere zu stören, oder während eines Computerspiels chatten wollen, sollten Sie am besten ein Headset verwenden (Abbildung 10.44). Headsets gibt es mit oder ohne Mikrofon. Sie verwenden die gleichen Anschlüsse wie Lautsprecher und Mikrofone. Headsets ohne Mikrofon verwenden meist den RCA-Anschluss, Headsets mit Mikrofon hingegen werden vorwiegend per USB angeschlossen – allerdings gibt es viele Ausnahmen von dieser Regel.

Viele Systeme verwenden inzwischen eigene USB-Geräte zur Aufnahme oder Wiedergabe von Audio. Abbildung 10.45 zeigt ein solches Aufnahmegerät, das Focusrite Scarlet 2 (links) und einen DAC (*Digital-Analog-Converter*) von Schiit zur Wiedergabe von Musik.

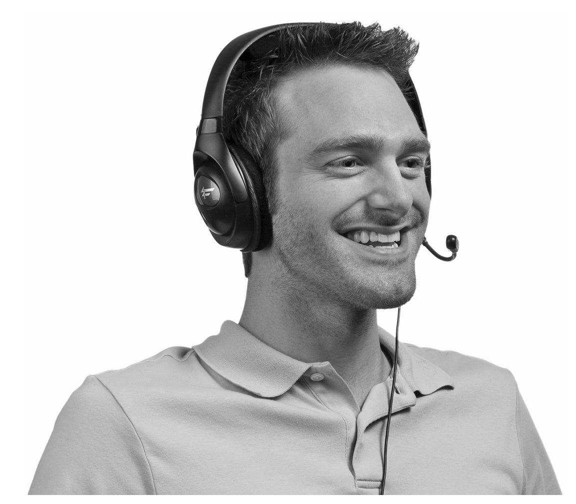


Abb. 10.44: Headsets sind bestens zum Spielen geeignet.



Abb. 10.45: Aufnahmegerät Scarlet und DAC von Schiit

10.2.11 Videoformate

Videodateien können sehr groß sein, deshalb betrachten wir kurz, wie sie gespeichert werden. Bei Audiodateien ist das noch vergleichsweise einfach. Sie entscheiden sich für ein Format wie AAC und speichern die Datei. Bei Videodateien ist das sehr viel komplizierter.

Videodateien bestehen aus zwei (oder mehr) eigenständigen Datenspuren (Bewegtbilder und Audio), die jeweils mit einem bestimmten Algorithmus komprimiert werden. Ansonsten bekämen Sie selbst bei kurzen Videos riesige Dateien. Dann werden die komprimierten Spuren in eine *Containerdatei* (oft auch *Wrapper* oder auch einfach nur *Container* genannt) verpackt. Wenn Sie in Standardcontainern (z.B. `.MOV` bei einem QuickTime-Film) verpackte Dateien erhalten, dann können Sie erst einmal nicht wissen, welche Codecs zur Komprimierung der in der Containerdatei enthaltenen Video- und Audiospuren verwendet wurden (Abbildung 10.46).

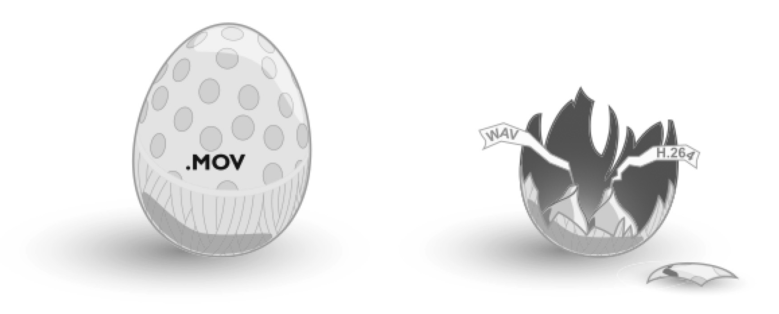


Abb. 10.46: Eine Containerdatei enthält mehrere Spuren, die jeweils separat codiert wurden.

Videocodecs Videodateien verwenden Standard-Audiocodecs für die Audiospuren, wie WAV oder MP3, unterscheiden sich aber stark hinsichtlich der verwendeten Videocodecs. Wie die Audiocodecs bei Audiodateien übernehmen auch Videocodecs einen Datenstrom (nur eben einen Videodatenstrom) und komprimieren ihn unter Verwendung verschiedener Algorithmen. Einige der standardisierten Videocodecs sind:

- *MPEG-2* (Part 2) wird für DVDs und Fernsehsendungen verwendet.
- *H.264* wird für alles Mögliche verwendet, vom Smartphone-Video über Streaming-Video bis hin zu Blu-ray-Filmen.
- *H.265* Die Dateien sind bei gleicher Qualität nur halb so groß wie H.264-Dateien. Unterstützt 4K-Video.
- *VP9* ist Googles Konkurrenz zu H.265. Wird auf Android-Geräten und bei YouTube verwendet.

Container Beim Komprimieren der Video- und Audioströme Ihrer Videodatei werden diese in irgendeiner Containerdatei abgelegt. Hier ist es wichtig zu wissen, dass Sie aus der Art der Containerdatei nicht unbedingt darauf schließen können, wie die Video- und Audiospuren komprimiert wurden. Sie können z.B. zwei scheinbar identische Videodateien vorliegen haben, die jeweils mit der Dateierweiterung `.MP4` gespeichert wurden, und müssen dann doch feststellen, dass bei der einen Video und Audio im Windows Media Player fehlerfrei wiedergegeben werden, während bei der anderen nur der Ton zu hören ist, weil dem Media Player der zur Wiedergabe des Videodatenstroms erforderliche Codec fehlt. Einige der Standardcontainer für Videos sind:

- *AVI* ist ein Container unter Windows, der heute kaum noch verwendet wird.
- *MOV* ist der Standardcontainer für Apple QuickTime.
- *MP4* ist das heute wohl am häufigsten verwendete Format, das für H.264- und H.265-Videos verwendet wird.

10.3 Speichergeräte

Die Bezeichnungen *Wechseldatenträger* und *Wechselmedien* beziehen sich auf beliebige Massenspeicher, die Sie in einem System benutzen, daraus physisch entnehmen und in einem anderen System benutzen können. Heutzutage sind Computer hochgradig vernetzt und Wechseldatenträger werden nur

noch vergleichsweise selten für den Transport von Programmen und Daten verwendet. Es gibt aber derart viele andere Verwendungszwecke dafür, dass sie weiterhin verbreitet sind. Wechseldatenträger sind das perfekte Medium zur Verteilung von Software, Datenarchivierung und Datensicherung.

Dieser Abschnitt des Kapitels behandelt die heute gebräuchlichsten Wechseldatenträger. Der Übersicht halber unterteile ich die Wechseldatenträger in die beiden folgenden Gruppen:

- **Flash-Speicher:** von USB-Sticks bis hin zu Flash-Speicherkarten
- **Optische Datenträger:** alle glänzenden Scheiben, von der CD-ROM über die DVD bis hin zur BD (Blu-ray-Disc)

Der obigen Beschreibung nach können Festplatten, SSDs oder optische Laufwerke, die extern an den PC angeschlossen werden, ebenfalls als Wechseldatenträger bezeichnet werden. Solche Laufwerke treten praktisch wie in den Kapiteln 8 und 9 beschrieben in Erscheinung und sind in dieser Hinsicht also nicht Neues.

10.3.1 Flash-Speicher

Derselbe *Flash-Speicher*, der die CMOS-Technologie beim System-BIOS ersetzt hat, findet auch in Form von Wechselmassenspeicher im PC Verwendung. Flash-Speicher gibt es in zwei verschiedenen Varianten, USB-Sticks und Speicherkarten. *USB-Sticks* sind kleine Flash-Geräte mit einem Standard-USB-Anschluss. *Speicherkarte* steht als Oberbegriff für all diese winzigen Kärtchen, die in Kameras, Smartphones und anderen Geräten eingesetzt werden. Beide Varianten können von modernen Betriebssystemen als Laufwerk genutzt werden, dienen aber meist anderen Aufgaben. USB-Sticks haben fast alle anderen wiederbeschreibbaren Wechselmedien ersetzt, wenn es darum geht, Dateien zu übertragen oder Kopien wichtiger Programme aufzubewahren. Meine Sticks (zwei davon habe ich immer bei mir) enthalten Sicherungskopien meiner aktuellen Arbeit, wichtige Fotos und einen Haufen Programme, die ich brauche, um Computer zu reparieren. Speicherkarten sind sehr klein und äußerst praktisch, wenn es darum geht, auf geringstem Raum Daten zu speichern, die auf einen PC übertragen werden sollen.

USB-Sticks

Daten zwischen verschiedenen Rechnern zu übertragen, war lange ziemlich mühsam. Heutzutage erfreuen sich *USB-Flash-Memory-Laufwerke*, die meist kurz *USB-Speichersticks* oder auch *RAM-Sticks* genannt werden, größter Beliebtheit (Abbildung 10.47). Ein 64 GB großer Speicherstick, auf den eine Menge Daten passen, ist schon für wenige Euro erhältlich.



Abb. 10.47: USB-Speichersticks

Bei den kleinsten Speichersticks ist der USB-Stecker bereits größer als der Speicher selbst, andere sind etwa so groß wie ein Feuerzeug. Diese Laufwerke lassen sich in allen modernen Betriebssystemen im laufenden Betrieb anschließen. Sie können das Laufwerk einfach mit einem USB-Anschluss verbinden, und schon wird es im Explorer oder auf dem Schreibtisch als Wechseldatenträger angezeigt. Nach der Verbindung mit dem USB-Anschluss können Sie die Daten vom USB-Laufwerk einfach auf die Festplatte kopieren oder dorthin verschieben, das Gerät wieder vom Rechner trennen und mitnehmen. Sie können Dateien direkt vom Laufwerk lesen, schreiben und löschen. Da es sich um USB-Geräte handelt, kommen die Speichersticks sogar ohne externe Stromversorgung aus. Da der Flash-Speicher aus Halbleiterbauteilen besteht, ist er unempfindlich gegenüber Erschütterungen und soll Daten etwa zehn Jahre lang aufbewahren können.

Neuere Rechner lassen sich sogar vom Speicherstick aus booten. Mit einem startfähigen Speicherstick können Sie bootfähige CDs und DVDs durch die schnelleren Flash-Laufwerke ersetzen. Die meisten Hersteller der klassischen bootfähigen CDs mit Dienstprogrammen USB-Versionen entwickelt und Programme erstellt, die vorhandene Speichersticks erkennen und ein Betriebssystem mit den gewünschten Dienstprogrammen darauf speichern können.

Hinweis

Denken Sie daran, im CMOS die Bootreihenfolge zu ändern, wenn Sie von einem USB-Speicherstick starten möchten. Ansonsten überspringt das BIOS den Speicherstick und lädt das normale Betriebssystem.

Flash-Karten

Flash-Karten erlauben die Speicherung von Daten auf kleinstem Raum. Es gibt sie in zahlreichen unterschiedlichen Formaten, deren gebräuchlichste Sie kennen sollten.

CompactFlash Bei *CompactFlash* (*CF*) handelt es sich um die älteste, komplexeste und physisch größte aller Flash-Speicherkarten (Abbildung 10.48). CF-Karten gibt es in zwei Größen: CF I (3,3 mm dick) und CF II (5 mm dick). CF-II-Karten sind zu dick für CF-I-Steckplätze.



Abb. 10.48: CF-Karte

SD-Karten (Secure Digital) Bei den *SD-Karten* (*Secure Digital*) handelt es sich um die heute gebräuchlichsten Flash-Datenträger. Die Medien in Größe kleiner Briefmarken gibt es in vielen Geräten mit Flash-Datenträger.

Die kleinen SD-Karten gibt es in zwei weiteren, kleineren Formaten: *MiniSD* (*Mini Secure Digital*) und *MicroSD* (*Micro Secure Digital*). MiniSDs werden kaum noch verwendet, aber MicroSDs sind bei Android-Smartphones und anderen kleinen Geräten enorm beliebt, die es ermöglichen, Speicher hinzuzufügen. Die geringe Größe erweist sich hier als Vorteil. Abbildung 10.49 zeigt die drei SD-Kartentypen.



Abb. 10.49: SD-, MiniSD- und MicroSD-Karten

SD-Karten gibt es mit drei Speicherkapazitäten. *Standard-SD*-Karten speichern zwischen 4 MB und 4 GB, *SDHC*-Karten (*Secure Digital High Capacity*) speichern zwischen 4 und 32 GB und die Speicherkapazität von *SDXC*-Karten (*Secure Digital Extended Capacity*) liegt zwischen 32 GB und 2 TB. Die älteren Lesegeräte für SD-Karten können keine SDHC- oder SDXC-Karten lesen, die neueren Standards sind aber abwärtskompatibel.

Wenn man herausfinden möchte, wie schnell eine bestimmte SD-Karte ist, wird es kompliziert. Die Geschwindigkeit spielt bei intensiver Nutzung eine Rolle, etwa bei der Aufnahme hochauflösender Videos ober bei der Hochgeschwindigkeitsfotografie.

Um es den Anwendern zu erleichtern, eine für ihren Bedarf hinreichend schnelle SD-Karte auszuwählen, haben die Hersteller verschiedene Standards zur Angabe der Leistung entwickelt. Diese Standards lassen sich grob in drei Generationen unterteilen. Bei Karten der ersten Generation wird eine Geschwindigkeitsklasse (2, 4, 6 oder 10) verwendet, die angibt, wie groß die minimale Schreibgeschwindigkeit in MB/s ist. Eine Karte der Klasse 10 sollte also mindestens 10 MB/s schreiben.

Die zweite Generation fiel mit der Vorstellung des neuen UHS-Busses (*Ultra High Speed*) zusammen. Die Karten verwenden den Standard *UHS Speed Class*; Karten der Klasse U1 sollten mit mindestens 10 MB/s lesen und schreiben, solche der Klasse U3 hingegen mit mindestens 30 MB/s.

Die dritte Generation heißt *Video Speed Class*. Sie ist dafür ausgelegt, die neuesten Videostandards wie 4K oder sogar 8K zu unterstützen. Die langsamste Klasse ist V6, die 6 MB/s unterstützt, die Klassen gehen aber bis zu V90, was eine Schreibgeschwindigkeit von 90 MB/s garantiert. Und als ob all das noch nicht verwirrend genug ist, werden auf den Karten mehr als eine (wenn nicht alle) der Bewertungen dieser Systeme zur Beurteilung der Geschwindigkeit angegeben.

Es kommt aber noch besser! Die genannten Geschwindigkeitsklassen garantieren, dass eine Karte kontinuierlich mit der angegebenen Rate (oder schneller) schreiben kann. Bewertungen wie diese sind entscheidend, um beurteilen zu können, ob eine Karte schnell genug für ein Gerät wie z.B. eine Videokamera ist. Aber heutzutage werden SD-Karten nicht nur in Videokameras, sondern auch in Smartphones verwendet. Hier kommt der Standard APC (*Application Performance Class*) ins Spiel. Der Standard definiert zwei Klassen: A1 und A2. Beide unterstützen eine minimale kontinuierliche Schreibgeschwindigkeit von 10 MB/s. Der Unterschied besteht darin, wie viele E/A-Operationen pro Sekunde (IOPS, *Input/Output Operations Per Second*) die Karte schafft. A1 liefert 1500 IOPS beim Lesen und 500 IOPS beim Schreiben, A2 hingegen 4000 IOPS beim Lesen und 2000 IOPS beim Schreiben. Diese Leistungskennzahlen spielen beim Schreiben einer Videodatei kaum eine Rolle, es ergibt sich jedoch ein haushoher Unterschied, wenn mehrere Smartphone-Apps gleichzeitig auf die Karte zugreifen.

Abgesehen von diesen Bewertungen ist auf der Karte oder der Verpackung oft eine maximale Lesegeschwindigkeit (in MB/s) angegeben. Das wurde eingeführt, als vor einigen Jahren für professionelle Anwender entwickelte Karten auf den Markt kamen, aber heute findet sich diese Angabe auf Karten unterschiedlichster Qualität. Und wenn Sie sich wundern, wieso nicht auch die maximale Schreibgeschwindigkeit angegeben ist, dann ist das eine sehr gute Frage. Die Schreibgeschwindigkeit ist zwar auf keiner der mir bekannten SD-Karten angegeben, sie findet sich bei Hochleistungs-SD-Karten jedoch üblicherweise in der Produktbeschreibung.

Aufgrund der großen Vielfalt können sich zwei SD-Karten gleicher Kapazität sowohl preislich als auch bei der Geschwindigkeit sehr voneinander unterscheiden. Deshalb ist es wichtig, die Eigenschaften einer Karte genau zu untersuchen, um kein Geld für nicht benötigte Geschwindigkeit zu verschwenden und um nicht feststellen zu müssen, dass das vermeintliche Schnäppchen für Ihre neue Profi-Videokamera zu langsam ist.

xD-Picture-Card Die proprietären *xD-Picture-Cards* (*Extreme Digital Picture Cards*, Abbildung 10.50) waren etwa halb so groß wie SD-Karten. Sie wurden fast ausschließlich in Digitalkameras der Firmen Olympus und Fujifilm verwendet. xD-Picture-Cards gab es in drei Varianten: Original, Standard (Typ M) und Hi-Speed (Typ H). Die Standardkarten sind langsamer als die Originalkarten, bieten aber mehr Speicherplatz. Fuji und Olympus setzen in ihren Kameras mittlerweile SD-Karten ein. xD-Karten finden sich nur noch in der CompTIA A+-Prüfung.

Wichtig

Einige hochwertige Kameras (insbesondere von Nikon) verwenden ein Kartenformat namens XQD, das eine sehr hohe Datenübertragungsrate und Speicherkapazitäten von 2 TB und mehr bietet. Dieses Format gehört *nicht* zur Prüfung und sollte nicht mit dem älteren und langsameren xD-Kartenformat verwechselt werden, das in der Prüfung vorkommen kann. XQD wird von CFExpress (das auch nicht zur Prüfung gehört) abgelöst, das NVMe statt PCI Express verwendet, um noch schnellere Übertragungen und geringere Latenz zu erzielen.



Abb. 10.50: xD-Karte

Kartenleser Egal, welchen Typ Flash-Speicher Sie auch einsetzen, Ihr PC benötigt immer einen Kartenleser, um direkt auf die Daten der Karte zugreifen zu können. Mittlerweile sind zahlreiche günstige USB-Kartenleser erhältlich (Abbildung 10.51). Viele PCs und Drucker besitzen eingebaute Kartenleser – praktisch, wenn Sie mal schnell die Bilder auf Ihrer Kamera bearbeiten oder ausdrucken möchten.



Abb. 10.51: USB-Kartenleser

Es spielt keine Rolle, welche Art von Flash-Speicher Sie verwenden, er verhält sich genauso wie alle anderen Massenspeichergeräte. Sie können Speicherkarten also formatieren und Dateien kopieren, verschieben und umbenennen.

10.3.2 Optische Datenträger

O*ptischer Datenträger* ist ein Oberbegriff für alle diese glänzenden Scheiben mit einem Durchmesser von 12 cm. Für die dazugehörigen Laufwerke wird entsprechend die Bezeichnung *optische Laufwerke* verwendet. In diesem Abschnitt werden optische Datenträger erläutert, wobei abschließend die Installation optischer Laufwerke detailliert beschrieben wird. Optische Laufwerke sind im Begriff, auszusterben (oder sind es schon). Man findet sie noch in älteren Computern und in der CompTIA A+-Prüfung. Merken Sie sich den Inhalt dieses Kapitels für die Prüfung, danach können Sie optische Laufwerke vergessen.

CD-, DVD- und Blu-ray-Datenträger und -Laufwerke gibt es in den unterschiedlichsten Varianten und Formen. *CD* steht für *Compact Disc*, einen Datenträger, der ursprünglich als Ersatz für die Vinylschallplatte entwickelt wurde, bevor Ronald Reagan zum US-Präsidenten gewählt wurde. Die *DVD* (*Digital Versatile Disc*) verdrängte zuerst im Bereich der Kaufvideos die VHS-Kassette und wurde dann – aufgrund ihrer höheren Kapazität – auch zu einem beliebten Speichermedium für Sicherungskopien. Die *Blu-ray-Disc* (BD) ist im Bereich der hochauflösenden Filme und 4K zum einzigen optischen Format geworden.

Abgesehen von den drei Oberbegriffen bezieht sich der Begriff des optischen Datenträgers auf zahlreiche Formatvarianten, wie z.B. CD-ROM, CD-R, CD-RW, DVD, DVD+RW, HD-DVD, BD-R, BD-RE usw. All diese Technologien werden in diesem Kapitel noch eingehender beschrieben – hier sollten Sie nur wissen, dass es zwar viele verschiedene Formate für optische Datenträger gibt, dass es sich dabei physisch aber durchweg um diese kleinen, glänzenden Scheiben handelt.

CD-Datenträger

Am besten lassen sich optische Datenträger verstehen, wenn Sie erst einmal die vielen heute existierenden, verschiedenen Technologien vergessen und mit der guten alten CD (Compact Disc) in das Thema einsteigen. Alles Nachfolgende ist für die CompTIA A+-Prüfungen wichtig.

CDs speichern Daten durch die Verwendung mikroskopisch kleiner Vertiefungen (»Pits«), die durch einen leistungsstarken Laser auf einen gläsernen Master gebrannt werden. Kostspielige Maschinen stellen Kopien des gläsernen Masters aus Kunststoff her, die anschließend mit einer reflektierenden Metallschicht überzogen werden. CDs speichern nur auf einer Seite Daten. Das CD-Laufwerk liest die Vertiefungen und die nicht vertieften Flächen und konvertiert diese Muster in Nullen und Einsen.

CD-Formate Die ersten CDs wurden für die Musikwiedergabe entwickelt. Die Musikdaten wurden in einem speziellen Format abgelegt, das als *CDDA* (*CD-Digital Audio*) oder oft auch einfach als CD-Audio bezeichnet wird. CD-Audio unterteilt die Daten der CD in *Tracks* (Titel) variabler Länge, wobei auf Musik-CDs jedem Lied ein eigener Track zugeordnet wird. CD-Audio eignet sich zwar hervorragend zum Speichern von Tondaten, aber furchtbar schlecht für das Speichern von Daten, da keine Fehlerprüfung stattfindet und dafür geeignete Verzeichnisstrukturen fehlen. Aus diesem Grund entwickelten kluge Köpfe ein Verfahren, um Daten auf CDs zu speichern, das *CD-ROM* genannt wird. Das CD-ROM-Format unterteilt die CD in feste Sektoren, die jeweils 2.353 Byte Daten enthalten.

Im ersten Moment werden Sie vielleicht denken, »Warum verwenden CD-ROMS nicht einfach ein FAT- oder ein NTFS-Format wie Festplatten?« Natürlich könnten sie das! Es gibt kein physikalisches Gesetz, das es verhindern könnte, dass für die CD-ROM ein beliebiges Dateisystem verwendet wird. Die CD-Hersteller wollten aber nicht, dass die CD-ROM ein Dateiformat von Microsoft oder Apple oder irgendeines anderen Herstellers verwendet. Darüber hinaus sollten nicht nur PCs CDs lesen können. Deshalb wurde ein eigenes Dateisystem für CD-ROMs entwickelt, nämlich *ISO-9660*. Dieses Format wird manchmal auch allgemeiner *CDFS* (*CD File System*) genannt. Die allermeisten CD-ROMs verwenden heute dieses Format.

CD-ROM-Geschwindigkeiten Die ersten CD-ROM-Laufwerke konnten Daten mit ca. 150.000 Byte/s (150 KB/s) verarbeiten und arbeiteten damit mit der Geschwindigkeit des ursprünglichen CD-Audio-Formats. Obwohl diese Geschwindigkeit für Musik völlig ausreicht, erkannte die CD-ROM-Industrie schnell, dass die Installation von Programmen oder die Übertragung von Daten von einer CD-ROM mit 150 KBps das elektronische Pendant zur Beobachtung trocknender Farbe war. Seit dem Erscheinen der ersten CD-ROM-Laufwerke gibt es das Bestreben, sie schneller zu machen, um den Datendurchsatz zu verbessern. Jede Geschwindigkeitssteigerung wird in Vielfachen der ursprünglichen 150-KBps-Laufwerke angegeben, wobei der Multiplikator für die Geschwindigkeit im Verhältnis zu den ersten Laufwerken (1x) steht. Es folgt eine Liste der verbreiteten CD-ROM-Geschwindigkeiten, wobei Geräte mit den aufgeführten frühen Geschwindigkeiten heute nicht mehr hergestellt werden:

1x	150 KBps	24x	3600 KBps
2x	300 KBps	36x	5400 KBps
4x	600 KBps	48x	7200 KBps
16x	2400 KBps	72x	10800 KBps

CD-R Für die Herstellung von CD-ROMs sind eine spezielle, teure Ausrüstung und beträchtliche Kenntnisse erforderlich, sodass die CD-ROM-Produktion einer relativ kleinen Zahl von Herstellern vorbehalten bleibt. Seit den Tagen der ersten Marktvorstellung der CD-ROM gab es jedoch eine riesige Nachfrage nach Möglichkeiten für den normalen PC-Anwender, eigene CD-ROMs zu »brennen«.

Mitte der 1990er stellte die CD-Industrie den *CD-R*-Standard (*CD Recordable*) vor, der preiswerte CD-R-Laufwerke möglich machte, die häufig *CD-Brenner* genannt werden, mit denen Daten auf spezielle CD-R-Discs geschrieben werden konnten. Alle CD-ROM-Laufwerke können die auf CD-R gespeicherten Daten lesen und alle CD-R-Laufwerke können gewöhnliche CD-ROMs lesen. CD-R-Discs gibt es in zwei Varianten. Auf 74-Minuten-Discs lassen sich ca. 650 MB und auf 80-Minuten-Discs ca. 700 MB speichern (Abbildung 10.52). CD-R-Brenner müssen speziell für das 80-Minuten-CD-R-Format entwickelt worden sein, um dieses Format unterstützen zu können, was bei neuen CD-R-Laufwerken aber durchweg der Fall sein sollte.



Abb. 10.52: Ein CD-R-Datenträger mit Kapazitätsangabe

Die Funktionsweise der CD-R-Discs ähnelt derjenigen herkömmlicher CD-ROMs, auch wenn die bei ihrer Herstellung eingesetzten Chemikalien bei vielen CD-R-Discs für mehr Farbenpracht sorgen. Bei CD-ROM-Discs ist die Aufzeichnungsseite im Gegensatz dazu immer eintönig silberfarben. CD-R-

Laufwerke nutzen zur Datenaufzeichnung spezielle organische Farbstoffe (dyes), die in die Disc eingebettet sind. Diese Farbstoffe sind bei der CD-R auch für die verschiedenartigen Färbungen der Unterseite verantwortlich. CD-R-Brenner verfügen über einen zweiten »Brenn-Laser«, der mit etwa der zehnfachen Energie des Lese-Lasers arbeitet. Er erhitzt den organischen Farbstoff so, dass sich die Reflexion der Oberfläche ändert und damit funktional den Pits der CD-ROM entspricht.

Bei CD-R-Laufwerken spielen zwei Geschwindigkeiten eine Rolle: die Aufzeichnungs- und die Lesegeschwindigkeit. Beide Geschwindigkeiten werden in Vielfachen der 150 KB/s der ursprünglichen CD-ROM-Laufwerke angegeben. Die Aufzeichnungsgeschwindigkeit, die immer als Erstes angegeben wird, ist immer kleiner oder allenfalls gleich der Lesegeschwindigkeit. Entsprechend brennt ein CD-R-Laufwerk mit der Angabe 8x/24x Daten mit maximal 8x- und liest sie mit maximal 24x-Geschwindigkeit.

CD-RW CD-R-Laufwerke konnten CD-R-Discs brennen und CD-ROMs lesen. Aber es erschien ein neuer Laufwerktyp mit der Bezeichnung *CD-RW* (*CD-ReWritable*), der die älteren CD-R-Laufwerke abgelöst hat. Es gibt spezielle CD-Medien, die sogenannten CD-RWs, die mit diesen Geräten gebrannt und anschließend wieder gelöscht werden können. CD-RW-Laufwerke können auch CD-Rs schreiben, die sehr viel preisgünstiger sind.

Mit der CD-RW-Techologie können Sie nicht nur Discs brennen, sondern auch Daten *überschreiben*, die sich bereits auf CD-RW-Discs befinden. Durch das CD-RW-Format (*CD ReWritable*) wird das Medium CD letztlich im Grunde genommen zu einem 650-MB-RAM-Stick. Auch hier unterscheiden sich CD-RW-Discs äußerlich nicht von CD-ROM-Discs, wenn man einmal von der etwas anderen Färbung der Unterseite absieht. Abbildung 10.53 zeigt alle drei CD-Formate.



Abb. 10.53: CD-ROM-, CD-R- und CD-RW-Discs

Bei der CD-RW wird eine amorphe (nichtkristalline) Substanz mit einem Laser erhitzt, die nach dem Abkühlen langsam auskristallisiert. Die kristallinen Bereiche reflektieren, während das bei den amorphen Bereichen nicht der Fall ist. Da sowohl CD-R- als auch CD-RW-Laufwerke einen starken Laser erfordern, war die Herstellung von Laufwerken, die sowohl CD-Rs als auch CD-RWs brennen konnten, relativ einfach, sodass herkömmliche CD-R-Laufwerke fast von einem Tag auf den anderen vom Markt verschwanden. Warum sollte man auch noch ein CD-R-Laufwerk kaufen, wenn CD-RW-Laufwerke bei vergleichbarem Preis sowohl CD-R- als auch CD-RW-Discs beschreiben konnten?

Bei CD-RW-Laufwerken werden drei Multiplikatoren angegeben. Der erste steht für die CD-R-Schreibgeschwindigkeit, der zweite für die CD-RW-Schreibgeschwindigkeit und der dritte für die Lesegeschwindigkeit. Bei den Geschwindigkeiten für das Schreiben, Wiederbeschreiben und Lesen gab es teilweise erhebliche Unterschiede zwischen den verschiedenen CD-RW-Laufwerken, sodass es sich bei den folgenden Angaben lediglich um ein paar repräsentative Beispiele handelt: 8x4x32, 12x10x32 und 48x24x48.

Windows und CD-Medien Praktisch alle optischen Laufwerke haben die gleiche Schnittstelle wie ihre Massenspeichergeräte. Sie können ein Laufwerk also einfach anschließen, und wenn man dabei keine Fehler gemacht hat, wird es unter Windows angezeigt (Abbildung 10.54).

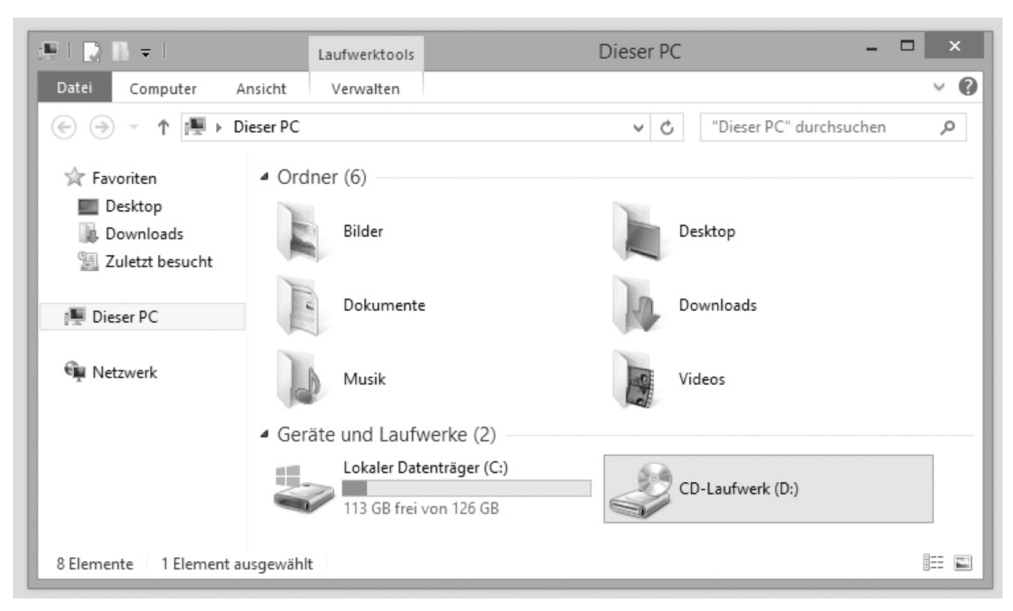


Abb. 10.54: Optisches Laufwerk in Windows

DVD-Datenträger

Jahrelang hat die Videoindustrie versucht, ein CD-Medium zu schaffen, das die Videokassette ersetzen sollte. Die DVD wurde in den frühen 1990ern von einem großen Firmenkonsortium aus dem Elektronik- und Unterhaltungsbereich entwickelt und 1995 als *Digital Video Disc* auf den Markt gebracht. Durch die Wandlung der DVD zu einem Datenspeichermedium wurde schon bald eine Namensänderung erforderlich, sodass DVD nun für *Digital Versatile Disc* steht.



Abb. 10.55: Eine typische Video-DVD

Es werden aber weiterhin beide Begriffe verwendet. Die Branche verwendet zudem noch die Bezeichnung *DVD-Video*, um das Filmformat von den Datenformaten zu unterscheiden. Sieht man einmal von dem auf allen kommerziellen DVDs aufgedruckten DVD-Logo ab (Abbildung 10.55), sehen DVD-Discs äußerlich genau wie alle anderen Compact-Disc-Medien aus. Damit enden die Ähnlichkeiten aber auch schon.

Am besten lässt sich die DVD über ihre Kapazität beschreiben. Die DVD-Variante mit der niedrigsten Kapazität fasst bereits 4,37 GB Daten oder zwei Stunden Video im Standardformat. Auf DVD-Discs mit der höchsten Kapazität lassen sich ca. 16 GB Daten oder acht Stunden Video speichern! Die DVD erreicht diese erstaunlichen Kapazitäten mit einer Reihe von Technologien, von denen drei besonders wichtig sind. Erstens sind die Pits auf DVDs kleiner und viel dichter als auf CDs gepackt. Zweitens gibt es von der DVD sowohl einseitige (*SS – Single-Sided*) als auch zweiseitige (*DS – Double-Sided*) Formate. Natürlich passen auf DS-Discs doppelt so viele Daten wie auf SS-Discs, diese müssen aber auch gewendet werden, wenn die zweite Seite gelesen werden soll. Drittens gibt es von den DVD-Discs einlagige (*SL – Single-Layer*) und zweilagige (*DL – Dual-Layer*) Formate. DL-Discs arbeiten mit zwei Pit-Schichten je Seite, wobei die zweite Schicht einen etwas abweichenden Reflexionswert aufweist. Tabelle 10.3 führt die Kapazitäten der verschiedenen DVD-Discs auf.

DVD-Variante	Kapazität
DVD-5 (12 cm, SS/SL)	4,37 GB Daten, ca. 2 Stunden Video
DVD-9 (12 cm, SS/DL)	7,95 GB Daten, ca. 4 Stunden Video
DVD-10 (12 cm, DS/SL)	8,74 GB Daten, ca. 4,5 Stunden Video
DVD-18 (12 cm, DS/DL)	15,90 GB Daten, ca. 8 Stunden Video

Tabelle 10.3: Kapazitäten der verschiedenen DVD-Varianten

DVD-ROM *DVD-ROM* ist das DVD-Äquivalent des Standard-CD-ROM-Datenformats, nur dass sich hier bis zu (fast) 16 GB speichern lassen. Nahezu alle DVD-ROM-Laufwerke unterstützen neben DVD-Video auch die meisten CD-ROM-Formate. Die meisten zusammen mit einem PC verkauften Laufwerke sind DVD-ROM-Laufwerke.

Recordable DVD Die IT-Industrie hat nicht weniger als *drei* verschiedene Standards beschreibbarer DVD-Medien entwickelt: DVD-R, DVD-RW und DVD-RW DL. DVD-R-Discs funktionieren wie CD-Rs. Sie können Daten darauf schreiben, die später nicht mehr gelöscht oder geändert werden können. Eine DVD-R DL kann auf beiden Seiten beschrieben werden und verdoppelt damit die Kapazität. DVD-RW-Discs können, wie CD-RW-Discs, gelesen und wiederholt beschrieben werden. Die meisten DVD-Laufwerke können alle Formate lesen.

Wichtig

In den Lernzielen der CompTIA A+-Zertifizierungsprüfung werden Discs des Typs DVD-RW DL als gebräuchliches beschreibbares Medium genannt. Die Spezifikation ist schon einige Jahre alt, die Medien sind jedoch praktisch kaum in Gebrauch. Die verschiedenen DVD-Typen sind inzwischen von Blu-ray-Discs überholt worden.

Blu-ray-Disc

Die Blu-ray-Disc ist die jüngste Generation in der Entwicklung der Speichertechnik der optischen Disc (Abbildung 10.56). Aufgrund der nahezu perfekten Audio- und Videoqualität, der breiten Akzeptanz durch die führenden Unternehmen im Computer-, Elektronik-, Spiele- und Musikbereich, durch Einzelhandel und Filmproduzenten und die hohe Speicherkapazität von bis zu 25 GB (einschichtige Disc), 50 GB (doppelschichtige Disc) bzw. 100 GB (BDXL) erfreute sich die Blu-ray-Disc außerordentlicher Beliebtheit, bis Flash-Speichermedien in den 2010er-Jahren so preiswert wurden, dass sie praktisch alle optischen Datenträger verdrängt haben.

Wichtig

Apple hat schon vor geraumer Zeit aufgehört, in Desktops und Laptops optische Laufwerke einzubauen. Da manche Benutzer nicht auf optische Medien verzichten möchten, hat Apple in macOS eine Funktion namens »Entfernte CD/DVD« eingebaut, mit der es möglich ist, optische Medien in Laufwerken anderer Systeme zu lesen.

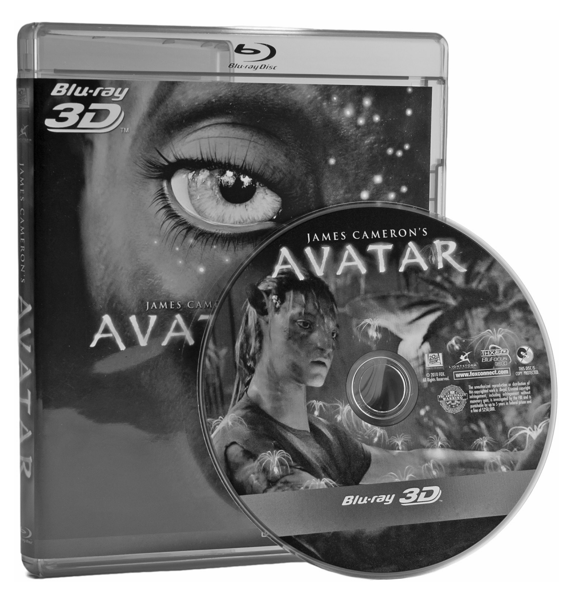


Abb. 10.56: Blu-ray-Disc im Standardformat

Hinweis

Falls Sie eine Xbox One bzw. eine Playstation 3 (oder ein neueres Modell) besitzen, verfügen Sie auch über einen Blu-ray-Player, denn dieses Format verwenden die optischen Laufwerke der Spielkonsolen.

BD-ROM Bei der *BD-ROM* (nur lesbar) handelt es sich um das Blue-ray-Pendant zum DVD-ROM-Standardformat, nur dass auf die entsprechenden Scheiben viel mehr Daten passen, die für eine höhere Audio- und Videoqualität ausreichen. Die allermeisten BD-ROM-Laufwerke sind voll abwärtskompatibel und unterstützen neben DVD-Video auch die meisten CD-ROM-Formate. Wenn Sie sich Filme auf Ihrem HDTV-Fernseher in bestmöglicher Qualität ansehen wollen, dann sollten Sie sich einen Blu-ray-Player anschaffen und Blu-ray-Discs anstelle von DVDs verwenden. Bei den heutigen Rechnern sind standardmäßig meist keine optischen Laufwerke installiert. Sie können aber meist Systeme mit Blu-ray-Laufwerken bestellen oder einfach selbst ein solches Laufwerk installieren. Abbildung 10.57 zeigt ein Blu-ray-Laufwerk.

BD-R und BD-RE Bei Blu-ray-Discs gibt es zwei beschreibbare Formate, die *BD-R* (für »recordable«) und *BD-RE* (für »rewritable«) genannt werden. Eine BD-R lässt sich ein einziges Mal beschreiben. Eine BD-RE lässt sich mehrfach beschreiben und löschen. Auch von BD-R und BD-RE sind Mini-Blu-ray-Discs erhältlich.



Abb. 10.57: Ein Blu-ray-/DVD-/CD-Kombilaufwerk

Optische Laufwerke installieren

Aus drei Meter Abstand sehen alle optischen Laufwerke absolut gleich aus. Abbildung 10.58 zeigt ein CD-RW-, ein DVD- und ein BD-R-Laufwerk. Können Sie die Laufwerke auf den ersten Blick unterscheiden? Falls Sie noch rätseln: Das CD-RW-Laufwerk befindet sich unten, das DVD-Laufwerk in der Mitte und das BD-R-Laufwerk oben. Wenn Sie die Laufwerke näher betrachten, geben sie meist mittels eines kleinen Aufdrucks an der Vorderseite oder eines Aufklebers auf ihrem Gehäuse Auskunft über ihre Funktion (Abbildung 10.59).



Abb. 10.58: CD-RW-, DVD- und BD-R-Laufwerke

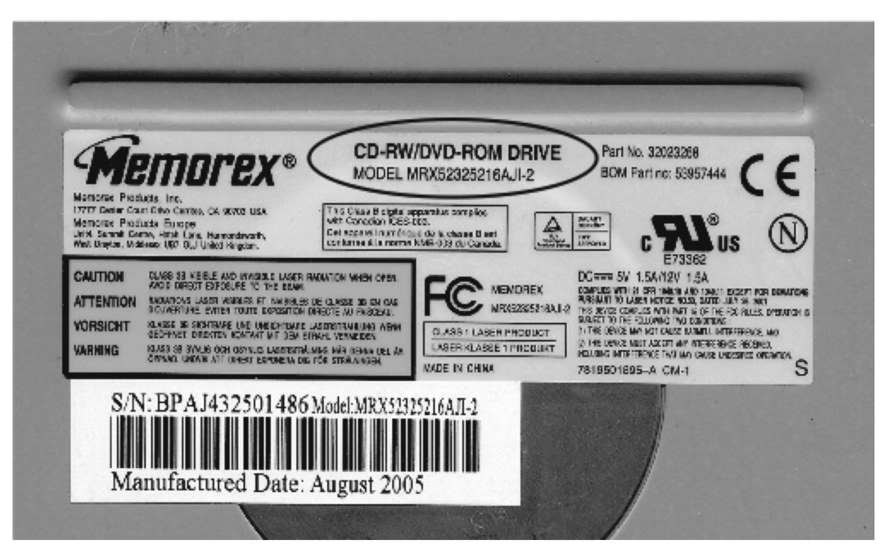


Abb. 10.59: Aufkleber auf einem optischen Laufwerk, der über Modell und Geschwindigkeit Auskunft gibt

Die meisten internen optischen Laufwerke verwenden SATA-Anschlüsse. Für externe optische Laufwerke werden meist USB- oder Thunderbolt-Anschlüsse verwendet.

10.4 Wiederholung

10.4.1 Fragen

1. Hans hat seiner Firma vorgeschlagen, die in den Smartphones des Unternehmens verwendeten SD-Karten des Typs 32 GB SDHC A1 durch Karten des Typs 128 GB SDXC A2 zu ersetzen. Was bedeutet A2?
   A. A2-Karten bieten eine deutlich größere Kapazität als A1-Karten.
   B. A2-Karten bieten eine deutlich höhere kontinuierliche Schreibgeschwindigkeit als A1-Karten.
   C. A2-Karten sind bei gleicher Leistung erheblich preiswerter als A1-Karten.
   D. A2-Karten bieten mehr IOPS als A1-Karten.
2. Was passiert mit der Busgeschwindigkeit und dem Stromverbrauch, wenn Sie mehrere Geräte an einen USB-Hub anschließen?
   A. Die Busgeschwindigkeit bleibt gleich, aber der Stromverbrauch steigt an.
   B. Die Busgeschwindigkeit steigt, weil jedes Gerät mit eigenen Spitzenraten arbeitet, der Stromverbrauch steigt.
   C. Die Busgeschwindigkeit sinkt, weil sich alle Geräte die Gesamtbandbreite teilen, der Stromverbrauch steigt.
   D. Die Busgeschwindigkeit sinkt, weil sich alle Geräte dieselbe Gesamtbandbreite teilen, der Stromverbrauch sinkt.
3. Welcher Anschlusstyp bietet die höchste Transferrate?
   A. IEEE 1394a
   B. SuperSpeed USB
   C. Full-Speed USB
   D. Hi-Speed USB

4. Ein Benutzer beschwert sich telefonisch bei Ihnen darüber, dass er die Fehlermeldung »Hub power exceeded« (Hub-Stromversorgung überschritten) erhält, wenn er seinen neuen USB-Stick mit dem externen USB-Anschluss der Tastatur verbindet. Außerdem funktioniert das Gerät nicht. Was ist die wahrscheinlichste Ursache des Problems?
   A. Sein USB-Anschluss ist defekt.
   B. Der USB-Stick ist defekt.
   C. Er hat ein Hi-Speed-Gerät in einen Full-Speed-Anschluss gesteckt.
   D. Er hat zu viele Geräte an den USB-Hub angeschlossen.
5. Welche nominelle Höchstgeschwindigkeit unterstützt der Hi-Speed-Modus von USB 2.0?
   A. 12 Mbps
   B. 120 Mbps
   C. 400 Mbps
   D. 480 Mbps
6. Welche maximale Kabellänge gilt für USB 2.0?
   A. 1,2 Meter
   B. 1,2 Yard
   C. 5 Meter
   D. 5 Fuß
7. Wie viele Lautsprecher gibt es bei einer Dolby-Digital-5.1-Konfiguration?
   A. Fünf Lautsprecher und einen Subwoofer
   B. Sechs Lautsprecher und einen Subwoofer
   C. Sieben Lautsprecher und einen Subwoofer
   D. Acht Lautsprecher und einen Subwoofer
8. Woraus besteht der Inhalt einer MIDI-Datei?
   A. Audio
   B. Binärdaten
   C. MP3
   D. Text
9. Welches optische Medium bietet die größte Kapazität beim Schreiben und Überschreiben von Daten?
   A. DVD-R
   B. DVD+R DL
   C. BD-RE
   D. BD-RW
10. Jens hat ein Video namens `familienurlaub.avi` heruntergeladen, das ein Freund geteilt hat. Wenn er es in seinem Medienplayer öffnet, hört er zwar den Ton, sieht aber kein Bild. Wie lässt sich das Problem wahrscheinlich beheben?
   A. Der Medienplayer unterstützt keine AVI-Dateien. Er muss eine andere Software installieren.
   B. Er verwendet einen Mac; er muss die Datei unter Windows abspielen.
   C. Auf seinem Computer fehlt der passende Videocodec. Er muss die Codecs auf seinem Computer aktualisieren.
   D. Die Videodatei ist beschädigt. Sein Freund muss sie erneut mit ihm teilen.

10.4.2 Antworten

1. **D.** Die APC-Klassen A1 und A2 beziehen sich auf die IOPS-Rate der Karten, wobei A2 eine höhere Leistung erbringt als A1. Das spielt bei Smartphones, auf denen mehrere Apps laufen, eine entscheidende Rolle. SDHC und SDXC beziehen sich auf die Speicherkapazität einer Karte.
2. **C.** Die Busgeschwindigkeit sinkt, weil sich alle Geräte dieselbe Gesamtbandbreite teilen müssen, und der Stromverbrauch steigt.
3. **B.** SuperSpeed USB hat hier die Nase vorn.
4. **D.** Wie die Fehlermeldung schon sagt, benötigt der Speicherstick zu viel Energie, die der Hub nicht bereitstellen kann.
5. **D.** Der Hi-Speed-Modus von USB 2.0 unterstützt theoretisch eine maximale Transferrate von 480 Mbps.
6. **C.** USB 2.0 unterstützt eine maximale Kabellänge von fünf Metern.
7. **A.** Eine Dolby-Digital-5.1-Konfiguration besteht aus fünf Lautsprechern und einem Subwoofer.
8. **D.** Eine MIDI-Datei enthält Text.
9. **C.** Von den genannten Discs bietet BD-RE die größte Kapazität beim Wiederbeschreiben.
10. **B.** Wahrscheinlich fehlt auf dem System der passende Videocodec. Jens muss die Codecs auf seinem Rechner aktualisieren.

Der maßgeschneiderte PC 11

Themen in diesem Kapitel:

- Zusammenstellung der Komponenten eines PCs mit speziellen Aufgaben
- Windows installieren und aktualisieren
- Aufgaben nach Abschluss der Installation

Wir Techniker richten Computer ein. Wir reparieren sie natürlich auch, aber es gibt kaum eine bessere Gelegenheit, Ihre Kenntnisse, Fähigkeiten und technische Expertise zu zeigen, als beim Zusammenstellen eines PCs, der exakt den Bedürfnissen Ihres Kunden entspricht.

In diesem Kapitel kommt vieles von dem zusammen, was Sie in den vorhergehenden zehn Kapiteln gelernt haben und ich lege einen Schwerpunkt darauf, was einen ausgezeichneten Windows-Computer erst zu dem macht, was er ist: die Installation von Windows. Zunächst sehen wir uns Rechner mit speziellen Aufgaben an, wenden uns dann der Installation und Aktualisierung von Windows zu und beenden das Kapitel mit den Aufgaben, die nach der eigentlichen Installation von Windows anstehen.

1001

11.1 PCs mit speziellen Aufgaben

Heutzutage benötigt fast jeder einen Computer, um Arbeit erledigen zu können. Die Art des erforderlichen Computers wird dabei durch die ausgeübte Tätigkeit und die von der IT-Abteilung bereitgestellte Netzwerkanbindung festgelegt. In diesem Abschnitt geht es um die Überlegungen, die man anstellen sollte, wenn man die Komponenten für einen PC mit speziellen Aufgaben zusammenstellt, inklusive der Kompatibilität von Hardware und Software, der Erweiterbarkeit und Probleme bei der Entsorgung. Wir werden uns sieben maßgeschneiderte PC-Konfigurationen ansehen, die Ihnen eine Vorstellung davon vermitteln, welchen Szenarien Sie als Techniker begegnen können.

11.1.1 Voraussetzungen

Um bestimmte Aufgaben vernünftig erledigen zu können, ist es oft erforderlich, dass auch der PC eine spezielle Ausstattung erhält, beispielsweise wenn mit dem Computer Video- und Audiobearbeitung erledigt werden sollen. Der Kunde hat ein Budget vorgesehen und für die Aufgabe ein bestimmtes Softwarepaket im Sinn. Bei der Medienproduktion fällt die Wahl oft auf Adobe Premiere und Adobe After Effects, die beide Bestandteil der Adobe Creative Suite sind, die der Kunde durch Zahlung einer monatlichen Gebühr lizenzieren kann. Sehen wir uns doch einmal an, was es bei der Beschaffung neuer Hardware bzw. beim Upgraden vorhandener Hardware zu beachten gilt.

Beschaffung neuer Hardware

Wenn der Kunde komplett neue Hardware wünscht, ist die Sache unkompliziert. Johannes beispielsweise, der ein kleines Geschäft betreibt, möchte zwei spezielle Maschinen neu beschaffen: ein Speichersystem zum Speichern allgemeiner Daten und ein Mediencentersystem für die Eingangshalle. Folgen Sie den Empfehlungen in diesem Kapitel und erkunden Sie, welche Kompatibilitätsanforderungen die Hardware und das Betriebssystem erfüllen müssen, um die vom Kunden gewünschte Software zu betreiben.

Um eine bestimmte Windows-Version empfehlen zu können, müssen Sie die vorhandenen Features gegen die Bedürfnisse des Kunden abwiegen. Microsoft veröffentlicht drei frei verkäufliche Versionen, die auf die unterschiedlichen Anforderungen von Unternehmen und Privatleuten zugeschnitten sind. Home ist die preisgünstigste, Pro kostet mehr und Enterprise ist am kostspieligsten. Die Home-Version von Windows 10 ist für alle erdenklichen Anwendungen eines Mediencenters geeignet, wäre also passend für den Rechner in Johannes' Empfangshalle. Es sollte unbedingt ein 64-Bit-Rechner sein, damit mehr RAM genutzt werden kann.

Wenn es im Firmennetzwerk eine Domäne/Active Directory zur Handhabung des Netzwerkzugriffs und der Benutzerkonten gibt, sollten Sie die Pro- oder die Enterprise-Version empfehlen. (In Kapitel 19, *Lokale Netzwerke*, finden Sie Details zur Organisation des Netzwerks durch Arbeitsgruppen und Domänen.) Diese Versionen ermöglichen den Zugriff auf eine Domäne, was mit der Home-Version nicht möglich ist. Darüber hinaus erlauben die Pro- und die Enterprise-Versionen mit BitLocker und EFS (Encryption File System) zwei Optionen zur Verschlüsselung von Laufwerken und Daten, eine sehr viel bessere Zugriffskontrolle auf Dateien und Ordner. (Mehr zu diesen beiden Technologien finden Sie in Kapitel 13, *Benutzer, Gruppen und Berechtigungen*.) Und wenn Johannes' Büro Teil eines größeren Netzwerks ist, das mehrere Büros großräumig verbindet, bietet die Enterprise-Version mit *BranchCache* eine raffinierte Methode, um Anwendungen an mehrere Orte zu verteilen.

Wichtig

Sie sollten damit rechnen, das in der CompTIA A+-Prüfung 1002 Fragen zum Vergleich der Features verschiedener Windows-Versionen vorkommen. In Kapitel 2, *Der gläserne PC*, haben Sie bereits einen Überblick erhalten. In diesem Abschnitt kommen weitere Details hinzu. Sie sollten diese Vergleiche aber noch einmal durchgehen, nachdem Sie später im Buch mehr über Netzwerke erfahren haben. Notieren Sie sich, an dieser Stelle nachzulesen, wenn es um das Lernziel 1.2 der 1002-Prüfung geht.

Upgrade vorhandener Hardware

Wenn Kunden ihre bereits vorhandene Hardware einsetzen möchten, kann es heikel werden. Es folgt ein typisches Beispiel, bei dem es zu Problemen kommen kann. Maria betreibt ein kleines Geschäft und möchte ein paar Videos erstellen, um ihre Produkte zu vermarkten. Sie hat einen Arbeitsplatzrechner von Dell mit Windows 8.1, der sie vor einigen Jahren eine Menge Geld gekostet hat. Er verfügt über einen Intel-Core-i7-Prozesor der ersten Generation, 4 GB DDR3-RAM und eine 500 GB große Festplatte. Sie wissen (oder werden es wissen, nachdem Sie den Abschnitt *Arbeitsplatzrechner zur Multimedia-Bearbeitung* in diesem Kapitel gelesen haben), dass mehr Arbeitsspeicher und mehr Massenspeicher erforderlich sind, damit der Computer als A/V-Arbeitsplatzrechner vernünftig funktioniert. Jetzt müssen Sie eine Menge Fragen beantworten, bevor Sie das Upgrade in Angriff nehmen.

Welche Hardwareanforderungen stellt die Anwendungssoftware (in diesem Fall die Creative Suite)? Wie viel RAM benötigt die Software? Wie viel RAM unterstützt das vorhandene System? Ist das für dieses System erforderliche DDR3-RAM noch erhältlich? Wie viele Laufwerke welcher Größe können in das Gehäuse eingebaut werden? Unterstützt das Mainboard diese Laufwerke?

Was sind die Systemvoraussetzungen für die Anwendung? Kommt ein Intel-Core-i7-Prozessor der ersten Generation mit der aktuellen Programmversion zurecht? Falls nicht, können Sie die CPU upgraden, ohne ein Vermögen auszugeben? (CPUs für ältere Sockel sind tendenziell teurer als CPUs für aktuelle Sockel; so ist das, wenn Angebot und Nachfrage den Preis bestimmen.)

Was sind die Betriebssystemanforderungen der Anwendungssoftware? Kann man die aktuelle Creative Suite unter Windows 8.1 ausführen? Wenn nicht, wie kann man auf Windows 10 aktualisieren? Welche Vorlieben hat der Kunde hinsichtlich des Betriebssystems? Und was ist, wenn Maria dem Desktop von Windows 8.1 gegenüber der Benutzeroberfläche von Windows 10 den Vorzug gibt? Wie soll man in einer so ungewöhnlichen Situation vorgehen?

Und schließlich muss geprüft werden, ob es irgendwelche herstellerabhängigen Beschränkungen für die Komponenten von Dell oder das Betriebssystem gibt. Wann erreicht das System das *End-of-life-*

Datum, also den Zeitpunkt, ab dem der Hersteller die Hardware nicht mehr unterstützt? Gibt es seitens des Herstellers irgendwelche Beschränkungen für die Aktualisierung des Betriebssystems, beispielsweise bestimmte Features, die speziell für Windows 8.1 ausgelegt sind und unter Windows 10 nicht mehr funktionieren? Über all diese Fragen der Kompatibilität der Betriebssysteme müssen Sie sich Gedanken machen, bevor Sie dem Kunden eine Empfehlung geben können.

11.1.2 Arbeitsplatzrechner für bestimmte Aufgaben

In der CompTIA A+-Zertifizierungsprüfung 1002 werden die folgenden Typen von Arbeitsplatzrechnern unterschieden: Thick-Clients, Thin-Clients, Arbeitsplatzrechner mit virtuellen Maschinen, Spiele-PCs, CAD/CAM-Arbeitsplatzrechner, Computer zur Multimedia-Bearbeitung und NAS-Geräte (*Network Attached Storage*).

Thick-Clients

Mit *Thick-Clients* sind Computer gemeint, auf denen ein aktuelles Betriebssystem läuft und die alle möglichen Anwendungen ausführen können (Abbildung 11.1). Dieser PC-Typ sollte dem Großteil der Anforderungen von Leuten gerecht werden, die im Büro oder zu Hause einen Computer nutzen möchten. Die meisten, die den Begriff »PC« benutzen, denken dabei an einen Thick-Client. Er ist das Arbeitspferd des modernen Computerwesens.



Abb. 11.1: Typischer Thick-Client

Der Namensbestandteil »Thick« sagt nichts über die tatsächlichen Abmessungen des Computergehäuses aus. Damit ist vielmehr gemeint, dass er viele Aufgaben erledigen kann, auch wenn er nicht mit einem Netzwerk verbunden ist.

Ein Thick-Client hat alles, was er braucht, um seine Arbeit ohne Netzwerkverbindung zu erledigen. Auf der Festplatte befindet sich ein startfähiges Betriebssystem. Auf dem Computer sind verschiedene Anwendungen installiert. Sie können Briefe schreiben, eine Tabellenkalkulation verwenden, Spiele spielen oder Videos bearbeiten. Irgendwann möchte man natürlich auch eine E-Mail versenden, ein Dokument ins Internet hochladen oder ein Online-Spiel nutzen, aber im Allgemeinen können Sie die meiste Arbeit ohne eine Netzwerkverbindung erledigen.

Für einen vernünftigen Thick-Client ist entscheidend, dass die Hardware den Anforderungen an das Betriebssystem und den typischerweise in Büros oder Heimbüros genutzten Anwendungen gerecht wird. Für alle Betriebssysteme gibt es minimale Systemanforderungen. In Tabelle 11.1 sind die minimalen Systemanforderungen für Windows 10 aufgeführt.

Bauteil	**Anforderung**
CPU	1 Gigahertz (GHz) 32-Bit- (x86) oder 64-Bit-Prozessor (x64) oder schneller
Arbeitsspeicher	1 Gigabyte RAM (32-Bit) oder 2 GB RAM (64-Bit)
Festplatte	16 GB (32-Bit) oder 20 GB (64-Bit) freier Festplattenplatz
Grafik	Grafikkarte, die DirectX 9 und WDDM unterstützt
Netzwerk	Internetzugang

Tabelle 11.1: Minimale Systemanforderungen für Windows 10

Hierbei handelt es sich um die minimalen, nicht die optimalen Anforderungen. Die angegebenen Werte sind lächerlich niedrig. In der Branche heißt es: »Diese Anforderungen mögen ausreichen, um Windows *laufen* zu lassen, aber nicht, um es *rennen* zu lassen!« (Wir Nerds finden das komisch.) Sehen wir uns lieber die empfohlenen Systemanforderungen an. Es gibt nicht bei allen Betriebssystemen vom Hersteller empfohlene Systemanforderungen, deshalb stellen die in Tabelle 11.2 genannten meine persönliche Empfehlung für einen typischen Thick-Client mit Windows 10 dar.

Bauteil	**Empfohlene Anforderung** **32-Bit ist obsolet! Alles läuft mit 64-Bit!**
CPU	2 GHz oder schneller
Arbeitsspeicher	8 GB RAM
Festplatte	500 GB freier Festplattenplatz (HDD oder SSD)
Grafik	Grafikkarte, die DirectX 10 und WDDM unterstützt
Netzwerk	Internetzugang mit 50 Mbps Download-Geschwindigkeit

Tabelle 11.2: Empfohlene Systemanforderungen für Windows 10

Ein normaler Thick-Client sollte die empfohlenen Systemanforderungen für Windows erfüllen oder übertreffen und typische Büro- und Internetanwendungen (wie Webbrowser und E-Mail-Programm) bereitstellen.

Ubuntu Linux nennt sowohl minimale als auch empfohlene Systemanforderungen. Abbildung 11.2 zeigt einen Auszug der Wikipedia-Seite.

Hier ist eine kurze Zusammenfassung:

- Ein Thick-Client ist ein vollständiges System mit eigenem Betriebssystem und Anwendungen.
- Ein Thick-Client benötigt keine Netzverbindung, um zu funktionieren.
- Ein Thick-Client sollte die empfohlenen Systemanforderungen seines Betriebssystems erfüllen.

Systemvoraussetzungen [Bearbeiten | Quelltext bearbeiten]

Ubuntu wird offiziell auf den x86- und ARM-Architekturen unterstützt. Inoffiziell kann man Ubuntu auf den PowerPC- (ppc64el), SPARC- (sparc64) und PA-RISC-Architekturen zum Laufen bringen. Auf der x86-Architektur IA-32 (x86 ab 32-Bit) wird ab Ubuntu 19.10 allerdings nur noch die 64-Bit-Variante x64 (amd64) unterstützt.

Als minimale Hardware-Anforderungen wurden für 8.10 Ubuntu 256 Megabyte Arbeitsspeicher und ein Prozessor-Modell mit 500 Megahertz von Ubuntu selbst genannt.[32] Auf der Festplatte wird ein freier Speicherplatz von etwa 5 Gigabyte empfohlen, belegt werden rund 2,5 Gigabyte, zudem wird bei Updates temporär rund ein Gigabyte weiterer Platz benötigt. Diese Anforderungen änderten sich mit aktuelleren Versionen nur geringfügig.

Empfohlene Systemvoraussetzungen für Ubuntu 18.04[33]		
Hardware	**Desktop-Edition (mit Desktop-Umgebung)**	**Server-Edition (mit CLI)**
Prozessor	2 GHz Doppelkernprozessor	300 MHz
RAM	2 GB	256 MB
GPU	VGA ab 1024 × 768 Bildschirmauflösung	Grafikkarte und Monitor ab 640 × 480 Pixel
Datenspeicher	25 GB	1,5 GB

Abb. 11.2: Systemanforderungen für Ubuntu Linux

Thin-Clients

Ein *Thin-Client* ist ein Computer, der dafür ausgelegt ist, einen Großteil seiner Arbeitslast auszulagern. Dazu greift er auf leistungsfähige Server zurück und kann deshalb sogar ohne Festplatte auskommen und muss auch nicht unbedingt selbst Daten speichern. Oft erfüllen Thin-Client-Computer nur einen einzigen Zweck und dienen z.B. als Verkaufsautomaten oder Registrierkassen. Ein weiteres heutzutage gängiges Beispiel sind Arbeitsplatzrechner mit Büroanwendungen. Äußerlich kann ein Thin-Client einem Thick-Client durchaus ähneln, er belegt jedoch weniger Ressourcen und er ist daher preiswerter und kann leichter bereitgestellt werden. Außerdem erleichtert die zentrale Speicherung der Daten die Arbeit des Administrators. Abbildung 11.3 zeigt einen typischen Thin-Client.



Abb. 11.3: Thin-Client eines Büroarbeitsplatzes

Da klassische Thin-Client-Computer auf eine *Netzwerkverbindung* angewiesen sind, über die sie auf die Server zugreifen können, komme ich in den Kapiteln 18 bis 21, die Netzwerke zum Thema haben, auf sie zurück.

Hier ist wieder eine kurze Zusammenfassung:

- Thin-Clients speichern nur grundlegende Programme und dienen oft nur einem einzigen Zweck.
- Thin-Clients benötigen eine Netzwerkverbindung, um zu funktionieren, möglicherweise sogar zum Booten.
- Thin-Clients erfüllen die minimalen Systemanforderungen ihres Betriebssystems.

Arbeitsplatzrechner mit virtuellen Maschinen

Virtualisierung ist eine leistungsfähige Technologie, die den gleichzeitigen Betrieb mehrerer Betriebssysteme auf einem einzigen Computer ermöglicht. Mithilfe der Virtualisierung können verschiedene, leistungshungrige Anwendungen auf einem einzigen Computer zusammengelegt werden und dadurch Stellfläche, Energie und viel Rennerei einsparen. Auf Arbeitsplatzrechnern wird die Virtualisierung für gewöhnlich dazu verwendet, innerhalb des normalen, auf der Festplatte des Computers installierten Betriebssystems, ein anderes Betriebssystem auszuführen (Abbildung 11.4).

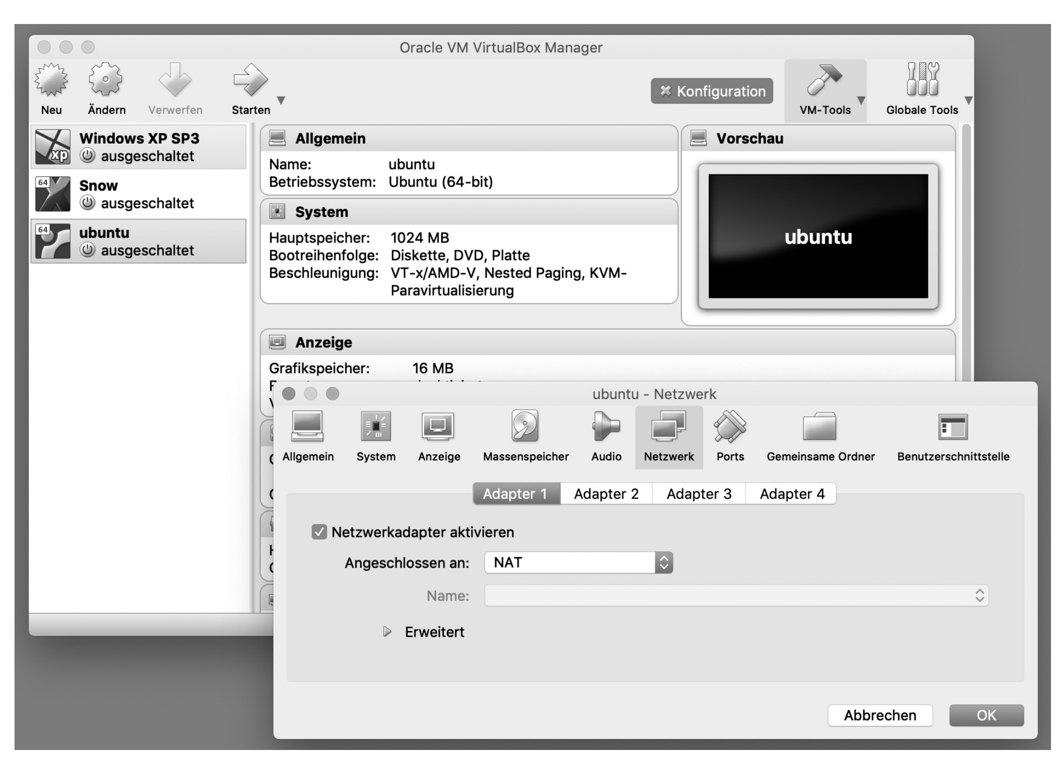


Abb. 11.4: VirtualBox auf einem macOS-System

Um auf einem Arbeitsplatzrechner mit virtuellen Maschinen eine akzeptable Geschwindigkeit zu erreichen, ist insbesondere viel RAM erforderlich. Ein solcher Rechner benötigt Arbeitsspeicher für den Betrieb des normalen Betriebssystems, den Betrieb der Gastbetriebssysteme und für alle Anwendungen, die auf den verschiedenen Betriebssystemen laufen, daher spielt die RAM-Ausstattung bei der Virtualisierung eine entscheidende Rolle. Ein leistungsfähiger 64-Bit-Prozessor mit vielen Prozessorkernen hilft ebenfalls dabei, einen reibungslosen Betrieb der virtuellen Maschinen zu gewährleis-

ten. Auf den meisten Desktop-Computern können virtuelle Maschinen ausgeführt werden, aber um die bestmögliche Leistung zu erzielen, sollte eine schnelle CPU und jede Menge Arbeitsspeicher eingesetzt werden.

Wichtig

Um auf einem Arbeitsplatzrechner mit virtuellen Maschinen eine anständige Leistung zu erzielen, ist eine schnelle CPU mit vielen Kernen und massenhaft Arbeitsspeicher erforderlich.

Zusammengefasst:

- Arbeitsplatzrechner mit virtuellen Maschinen benötigen möglichst viel RAM – nicht selten die maximal mögliche Menge.
- Arbeitsplatzrechner mit virtuellen Maschinen benötigen eine schnelle CPU mit so vielen Kernen, wie es das System (und Ihre Brieftasche) erlaubt.
- In Kapitel 22, *Virtualisierung*, werden wir uns virtuelle Maschinen ausführlich ansehen. Daher wird das Thema an dieser Stelle nicht vertieft.

Spiele-PCs

Computerspiele gehören zu den anspruchsvollsten Anwendungen für einen PC. Als aufstrebender Techniker haben Sie die ersten zaghaften Schritte auf der dunklen Schattenseite des PC vermutlich in einem Spiel unternommen: *Fortnite, Minecraft, Grand Theft Auto, Borderland 2, World of Warcraft* ... Sie haben doch sicher mindestens eines davon schon gespielt. Gelegenheitsspielern reicht ein normaler Desktop, wie der vorhin beschriebene Thick-Client-Computer, aber ernsthafte Spieler verlangen nach einem leistungsfähigen Spiele-PC, der die allerneuesten Grafikeffekte unterstützen kann.



Abb. 11.5: Der Spiele-PC des Autors (Steam-Accountname: desweds)

Ein echter Spieler setzt alle grafischen Einstellungen auf die Maximalwerte. Und da es beim Spielen nicht ausschließlich um die Optik geht, sollte es auch gern eine vernünftige Soundkarte und anstän-

dige Kopfhörer geben. (Nun gut, Sie brauchen natürlich auch ein vernünftiges Spiel, aber eins nach dem anderen.)

Eine hochwertige Grafikkarte mit leistungsfähiger *GPU* (Graphical Processing Unit) ist natürlich wichtig, aber nicht die einzige Aufrüstung, die erforderlich ist, damit die Spiele gut laufen. Sie brauchen einen schnellen Mehrkernprozessor, mehr Arbeitsspeicher als beim Thick-Client (minimal 16 GB, besser mehr) und eine erstklassige Soundkarte, die eine optimale räumliche Auflösung ermöglicht.

Wichtig

Eigenständige Soundkarten sind bei den heutigen Systemen ziemlich unwichtig. Sie finden die »Systemanforderung« für eine Soundkarte nur noch in der CompTIA A+-Prüfung.

GPUs haben wir noch nicht behandelt, dazu kommen wir in Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*. Inzwischen sollte aber klar sein, wie wichtig die hier genannten Komponenten sind. Erinnern Sie sich an die schnellsten CPUs aus Kapitel 3, *Mikroprozessoren*? So einen brauchen Sie – und eine leistungsstarke Kühlung, wie eine zweckmäßige Wasserkühlung. Damit haben Sie die Grundlage für einen erstklassigen Spiele-PC beisammen.

Zusammengefasst benötigt ein Spiele-PC:

- einen Mehrkernprozessor,
- eine leistungsfähige Kühlung (eventuell Wasserkühlung),
- eine hochwertige Grafikkarte und
- eine Soundkarte mit hoher räumlicher Auflösung.

Arbeitsplatzrechner zur Bildbearbeitung

Da professionelle Fotografen und Grafikdesigner im Allgemeinen mit sehr großen Dateien arbeiten, benötigen Arbeitsplatzrechner zur Bildbearbeitung einen schnellen Mehrkernprozessor, maximale RAM-Ausstattung und viel Speicherplatz. Da Designer visuell arbeiten, sind auch hochwertige Grafikkarten bei einem Arbeitsplatzrechner zur Bildbearbeitung unverzichtbar. Und schließlich nutzen professionelle Fotografen spezielle Software wie Adobe Photoshop oder Adobe Lightroom. Grafikern stehen noch einige weitere Optionen zur Verfügung, aber all diese Programme gehören zur Kategorie *CAD/CAM* (*Computer Aided Design/Computer Aided Manufacturing*).

Hinweis

CAD/CAM-Programme erlauben es Ingenieuren im industriellen Umfeld, Bauteile und Komponenten zu konstruieren und zu produzieren.

Für professionelle Fotografen und Grafikdesigner ist in erster Linie die bestmögliche Darstellung ihrer Fotografien und Bildbearbeitungswerkzeuge wichtig. Ob Sie nun in Adobe Lightroom die Bilder einer Hochzeit bearbeiten oder in *SolidWorks* eine technische Zeichnung erstellen, es muss sichergestellt sein, dass Sie auch genau sehen können, woran Sie arbeiten! Daher ist ein großer, hochwertiger Bildschirm bei einem Arbeitsplatzrechner zur Bildbearbeitung ein Muss. Ein LCD-Monitor vom Billigheimer für 150 Euro bringt Sie hier nicht weiter. Sie müssen schon gewährleisten können, dass die Farben auf dem Bildschirm so exakt wie nur möglich dargestellt werden.

In Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*, werden verschiedene hochwertige Komponenten behandelt, etwa IPS-Monitore und Grafikkarten, die mehrere Tausend Euro kosten. Dort werden wir mit der Betrachtung von Arbeitsplätzen zur Bildbearbeitung fortfahren. Zusammengefasst benötigt ein Arbeitsplatzrechner zur Bildbearbeitung:

- einen Mehrkernprozessor,
- eine hochwertige Grafikkarte mit GPU,

- sehr viel RAM (oft die maximal mögliche Menge) und
- reichlich Speicherplatz.

Arbeitsplatzrechner zur Multimedia-Bearbeitung

Als George Lucas den ersten Teil von *Star Wars* drehte, verwendete er Kameratricks, Miniaturmodelle und verschiedene Animationstechniken, um die Illusion gewaltiger Raumschiffe und kämpfender Roboter in einer weit entfernten Galaxie zu erzeugen. Zwanzig Jahre später fanden die Aufnahmen für die Vorgeschichte des Leinwandabenteuers vor einem riesigen grünen Hintergrund statt. Der nichtssagende grüne Hintergrund wurde mittels *CGI* (*Computer Generated Imagery*) durch exotische Planeten und Raumstationen ersetzt. Ich möchte gar nicht diskutieren, mit welcher Methode sich die besseren Filme produzieren lassen, aber es bleibt die Tatsache, dass sich die Art und Weise, wie Filme produziert werden, gewandelt hat. Und davon ist nicht nur das Kino betroffen, vielmehr hat der Einsatz von Computern auch die Entstehungsweise von Fernsehshows, Fotografien, Musik und anderem mehr verändert.

Wenn Sie an dieser Revolution teilhaben möchten, brauchen Sie einen richtig schnellen und leistungsfähigen Computer. Die Arbeitsplatzrechner für professionelle Bild-, Ton- und Videobearbeitung sind daher entsprechend gut ausgerüstet.

Digital Audio Workstation (DAW) Die Anforderungen an einen Arbeitsplatzrechner zur Audiobearbeitung, für den sich der Begriff DAW (Digital Audio Workstation) eingebürgert hat, sind denen bei der Bildbearbeitung sehr ähnlich – ein schneller Mehrkernprozessor, jede Menge RAM, ein großer Bildschirm sowie eine große und schnelle Festplatte. Der Unterschied besteht darin, dass darüber hinaus hochwertige Soundkomponenten notwendig sind.

Soundkarten im eigenen Gehäuse werden als *Audio-Interface* bezeichnet und sind in professionellen Umgebungen häufig anzutreffen. Das Audio-Interface ist üblicherweise ein kleines Kästchen, das Sie mit dem Computer verbinden und an das Sie professionelle Mikrofone und Musikinstrumente anschließen. Im Grunde genommen ist ein Audio-Interface eine hochwertige Soundkarte, die statt über einen Steckplatz auf dem Mainboard per USB mit dem Rechner verbunden wird. Es gibt Audio-Interfaces von der Größe einer Streichholzschachtel bis hin zu Geräten, die fast den gesamten Schreibtisch einnehmen. Die teureren Geräte besitzen mehr Anschlüsse und produzieren Klänge höherer Qualität. Um diese Unterschiede hören zu können, sind jedoch Lautsprecher entsprechender Qualität erforderlich.

Wie bei der Bildbearbeitung werden auch bei DAWs gern spezielle Eingabegeräte verwendet. Diese sogenannten *Control-Surfaces* ahmen häufig das Aussehen und die Funktion älterer analoger Mischpulte nach. Sie besitzen oft eine große Anzahl programmierbarer Eingänge, wodurch die Steuerung der zugehörigen Software nicht nur beschleunigt wird, sondern auch viel präziser als mit Maus und Tastatur erfolgt. Die Abmessungen von Control-Surfaces reichen von kleinen Tischgeräten bis zu raumfüllenden Kolossen, wie sie in Tonstudios verwendet werden. In manchen dieser Geräte ist auch noch ein Audio-Interface integriert.

Arbeitsplatzrechner zur Videobearbeitung Bei der Videobearbeitung sind die Anforderungen der Bild- und Audiobearbeitung miteinander kombiniert. Häufig werden beim Videoschnitt zwei oder mehr farbkalibrierte Bildschirme verwendet, sodass auf einem Monitor das eigentliche Video und auf einem anderen Bildschirm die Bearbeitungswerkzeuge angezeigt werden. Mehrere Bildschirme sind hier besonders hilfreich. Ein Rechner für die Videobearbeitung benötigt einen äußerst leistungsfähigen Prozessor und so viel RAM wie nur möglich, denn die Bearbeitung von Videomaterial ist ein Vorgang, der sehr viel rechenintensiver ist als die Bearbeitung von Fotos oder Audiodaten. Besonders schnelle und sehr große Festplatten sind ebenfalls unverzichtbar, da Videoprojekte oft viele Terabyte groß sind. Bei vielen Videoschnittplätzen kommen RAID-Verbunde zum Einsatz, um die Arbeitsgeschwindigkeit zu erhöhen und Speicherkapazität bereitzustellen.

Die Videobearbeitung profitiert – ebenso wie CAD/CAM – in sehr hohem Maße von Profi-Grafikkarten. Dies ist fast ebenso bedeutsam wie der schnelle Prozessor und massenhaft RAM. Sie werden kaum einen Videoschnittplatz finden, der keine solche Grafikkarte verwendet.

Da Arbeitsplatzrechner zur Videobearbeitung oftmals auch zur Audiobearbeitung eingesetzt werden, findet man bei ihnen häufig Audio-Interfaces und Control-Surfaces. Manche Systeme besitzen Videoschnittstellen, die es dem Bearbeiter ermöglichen, verschiedene Kameras anzuschließen. Viele Videobearbeiter verwenden auch spezielle Tastaturen, die zusätzliche Steuerelemente besitzen und eigens beschriftet sind, um die verbreiteten Videoschnittprogramme bequem bedienen zu können.

Wichtig

In den Lernzielen der CompTIA A+-Zertifizierungsprüfung werden Arbeitsplatzrechner zur Audio- und Videobearbeitung zusammen abgehandelt. Das liegt nahe, da solche Rechner oft beide Aufgaben übernehmen müssen und Sie sollten sich das für die Prüfung merken. In der Praxis begegnet man sowohl nur für Audio- bzw. nur für Videobearbeitung vorgesehenen Rechnern als auch solchen, die beide Aufgaben erledigen können.

Hier sind die Anforderungen für Arbeitsplatzrechner zur Multimedia-Bearbeitung zusammengefasst:

- Spezielle Sound- und Grafikkarten
- Große und schnelle Massendatenspeicher
- Sehr viel RAM, oft die maximal mögliche Menge
- Zwei (oder mehr) Bildschirme

11.1.3 NAS-Geräte

Wie viele Computer oder Computer-ähnliche Geräte gibt es in Ihrem Haushalt? Meine Antwort lautet: »Eine Menge.« Mehrere Smartphones, Geräte zum Medienstreaming, Spielkonsolen, Tablets und eine ganze Reihe Computer – da kommt schon einiges zusammen.

Wenn sich im Haushalt immer mehr Geräte ansammeln, gibt es schon bald Bedarf für einen zentralen Ort, an dem man Daten ablegen kann. Ein NAS-Gerät (*Network Attached Storage*), um Dateien und Ordner auf Wunsch bereitzustellen und um all Ihre Multimedia-Dateien aufzunehmen und diese an verschiedene Geräte zu streamen, ist dafür bestens geeignet. Die Anforderungen an ein solches NAS-Gerät sind aber schon so speziell, dass es sich deutlich vom herkömmlichen Thick-Client-Computer unterscheidet.

Ein NAS-Gerät muss drei verschiedene Aufgaben erledigen: Medienstreaming sowie die Freigabe von Ordnern und Druckern. Beim Medienstreaming kommt zwar oft hoch spezialisierte Software zum Einsatz, es funktioniert jedoch ebenso wie die Freigabe von Ordnern und Druckern mit den einschlägigen Programmen unter Windows und macOS problemlos. Das NAS-Gerät sollte über eine sehr schnelle Netzwerkanbindung und reichlich Speicherplatz verfügen, der außerdem fehlertolerant sein sollte. Der Verlust der Spielfilmsammlung durch den Ausfall einer Festplatte wäre wirklich mehr als ärgerlich.

Software

Alle modernen Betriebssysteme ermöglichen es, mit Bordmitteln Dateien und Ordner freizugeben. Gleiches gilt für Drucker. Um einen Computer zu einem Druckerserver zu machen, müssen Sie nur das Dialogfeld DRUCKEREIGENSCHAFTEN eines Druckers öffnen (über die App EINSTELLUNGEN oder über die Systemsteuerung) und auf der Registerkarte FREIGABE das Kontrollkästchen DRUCKER FREIGEBEN markieren (Abbildung 11.6).

Einen Windows-PC können Sie in einen Streaming-Server verwandeln, indem Sie die entsprechende Option in der Systemsteuerung aktivieren. Geben Sie in das Suchfeld der Taskleiste `Medienstreamingoptionen` ein und öffnen Sie diese (Abbildung 11.7).

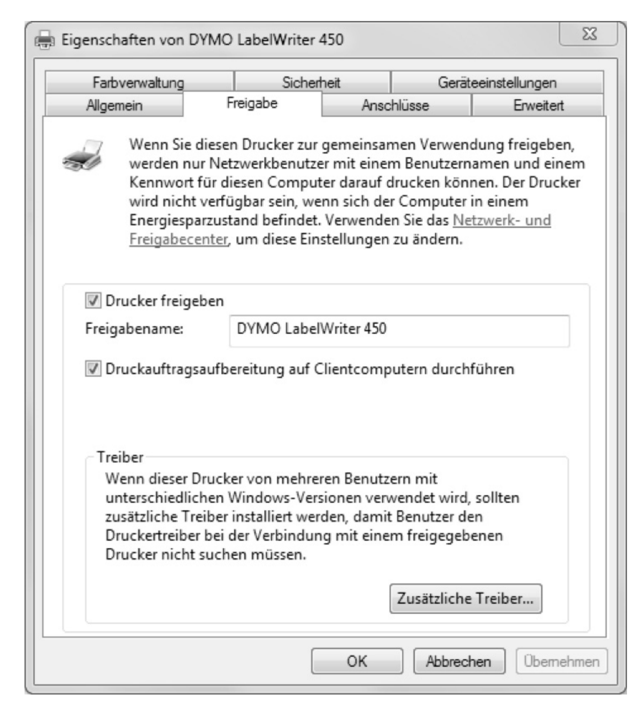


Abb. 11.6: Freigeben eines Druckers

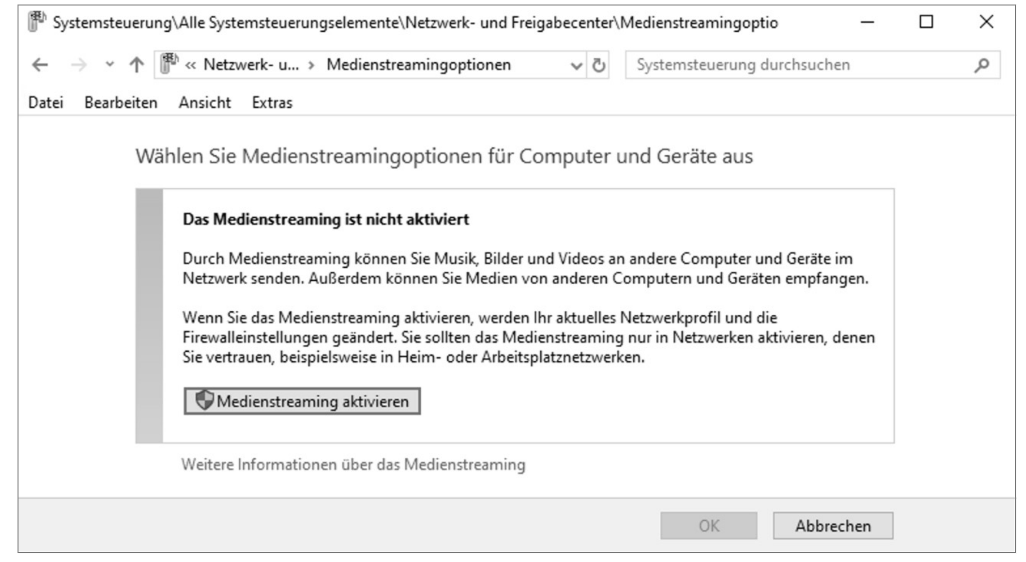


Abb. 11.7: Medienstreaming ist deaktiviert.

Nachdem Sie das Medienstreaming aktiviert haben, können Sie auswählen, mit welchen anderen Systemen Sie Ihre Streams teilen möchten (Abbildung 11.8). Standardmäßig möchte Windows alles freigeben, Sie haben aber die Möglichkeit, das zu ändern, falls Sie kleine Kinder haben und ihnen den Zugriff auf für sie ungeeignete Inhalte verwehren möchten.

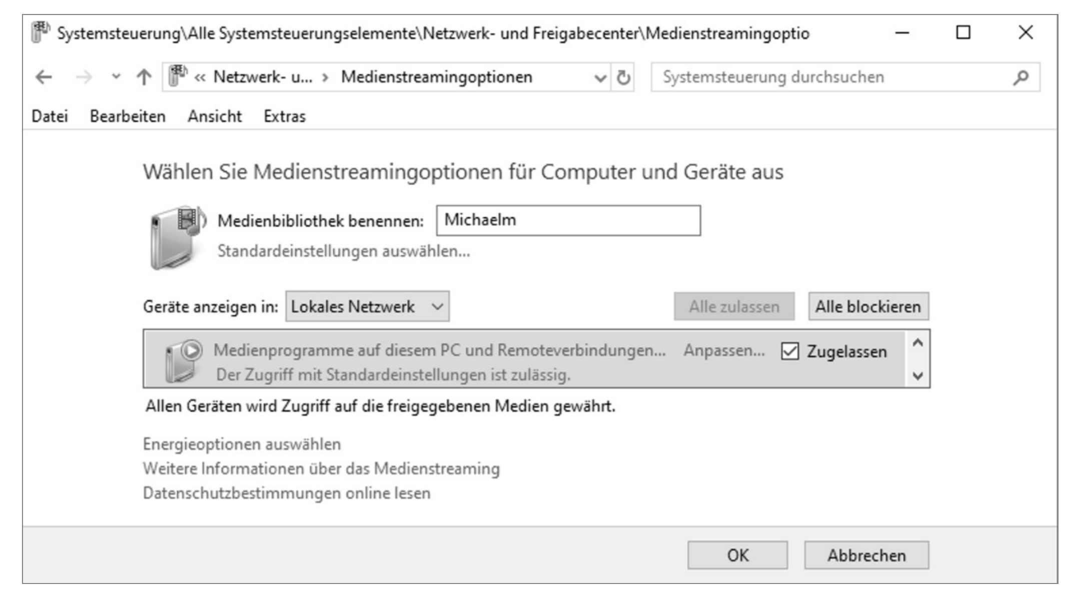


Abb. 11.8: Medienstreamingoptionen

Sowohl der Windows Media Player als auch iTunes ermöglichen es, Multimedia-Dateien im lokalen Netzwerk freizugeben. Abbildung 11.9 zeigt die Freigabe in iTunes via Bonjour.



Abb. 11.9: Streaming per iTunes

Hardware

Die Hardware-Anforderungen für ein NAS-Gerät beziehen sich vornehmlich auf die Geschwindigkeit des Netzwerks und die Fehlertoleranz der Festplatte, zumindest wenn man den Lernzielen der CompTIA Glauben schenkt. Bei einem sehr betriebsamen Server sollten Sie jedoch auch die RAM-Ausstattung und die CPU-Geschwindigkeit berücksichtigen. Rüsten Sie RAM und CPU auf, falls Sie bei der Geschwindigkeit Defizite feststellen.

Für die Netzwerkanbindung sollte kabelgebundenes Gigabit-Ethernet verwendet werden. Es ist zwar verführerisch, das drahtlos zu erledigen, aber besser ist es, ein drahtloses Netzwerk nur für die Verbindung zwischen Zugriffspunkt und Client zu verwenden. Durch die Verbindung per Ethernet-Kabel vermeiden Sie Verzögerungen durch Interferenzen und das Verlorengehen von Datenpaketen.

Die Festplatten eines Dateiservers verrichten dauerhaft Schwerstarbeit, sparen Sie hier nicht am falschen Ende. Beschaffen Sie mindestens zwei Laufwerke gleicher Größe mit möglichst großer Speicherkapazität. Und da Fehlertoleranz erforderlich ist, sollten Sie mindestens ein RAID 1 einrichten, weshalb die Festplatten auch von gleicher Größe sein sollten. Falls Ihr Budget es erlaubt und das Mainboard es unterstützt, ist es am besten, vier Laufwerke zu verwenden und einen RAID-10-Verbund einzurichten.

Wie Sie aus Kapitel 9 wissen, bietet Windows 8/8.1/10 die Möglichkeit, *Speicherplätze* und *Speicherpools* einzurichten, um eine beliebige Anzahl von Laufwerken zu einem Verbund zusammenzufassen. Wenn Sie beispielsweise einen Speicherpool mit drei 4-TB-Laufwerken erstellen und einen einzelnen Speicherplatz einrichten, haben Sie tatsächlich ein RAID 5 eingerichtet.

Zusammengefasst sollte ein NAS-Gerät Folgendes bieten:

- Freigabe von Ordnern
- Medienstreaming
- RAID-Verbund
- Gigabit-Ethernet

Tipp

Sehen Sie sich die Übung zu Kapitel 11 unter `http://totalsem.com/100x` an. Sie bestätigt, dass es für unterschiedliche Systeme verschiedene Anforderungen gibt.

1002

11.2 Windows installieren und aktualisieren

Nachdem Sie die Hardware für den neu einzurichtenden PC ausgewählt und beschafft haben, ist es an der Zeit, ein Betriebssystem zu installieren. Auf den meisten Computern werden Sie irgendeine Windows-Version installieren wollen. Und bei der jeweiligen Version müssen Sie die passende Edition auswählen. Dieser Abschnitt befasst sich mit der Auswahl der Installationsmedien, den verschiedenen Installationsmethoden und dann mit dem eigentlichen Installations- bzw. Aktualisierungsvorgang. Zum Abschluss werfen wir einen Blick auf die Behebung von Installationsproblemen.

Hinweis

Dieser Abschnitt erläutert die Installation für *Thick-Clients*, den typischen eigenständigen Windows-Systemen. Bei der Installation eines *Thin-Clients* wird ein Rechner am Netzwerk angeschlossen und gebootet. Anschließend sind nur minimale Konfigurationsarbeiten vorzunehmen. Die entscheidenden Vorgänge finden auf dem Server statt. In den Kapiteln 18 bis 21 werde ich ausführlicher darauf eingehen. Manche

Thin-Client-Implementierungen verwenden virtuelle Maschinen, die auf dem Server ausgeführt werden. Deshalb betrachten wir in Kapitel 22, *Virtualisierung*, auch Thin-Client eingehender.

11.2.1 Medienquellen

Grundsätzlich besteht eine Windows-Installation aus zwei Schritten. Zunächst einmal startet das System von einem Installationsmedium. Dann beantworten Sie Fragen des Installationsassistenten und lassen ihn seine Aufgabe erledigen. Nach Abschluss dieses 10 bis 40 Minuten in Anspruch nehmenden Vorgangs wird ein Begrüßungsbildschirm angezeigt (Abbildung 11.10). Nun können Sie sich in die Arbeit mit dem PC vertiefen.

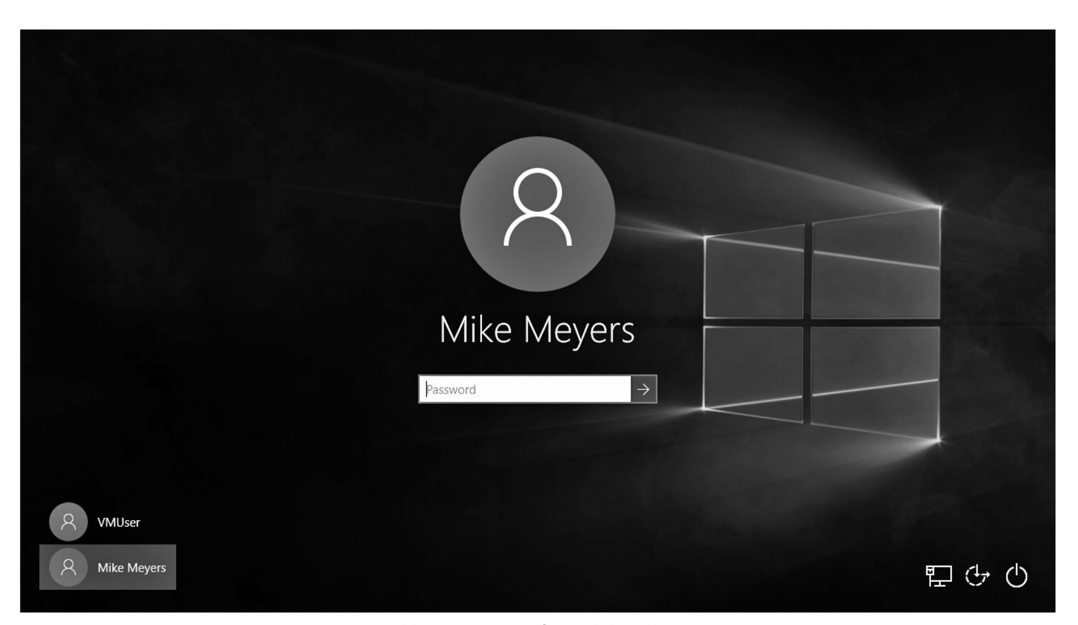


Abb. 11.10: Begrüßungsbildschirm

Wichtig

Nach einer erfolgreichen Installation ist das Startlaufwerk ordnungsgemäß partitioniert und formatiert.

Windows bietet eine erstaunlich große Anzahl verschiedener Startmethoden an. Bislang legte man meistens eine Windows-DVD in ein optisches Laufwerk, änderte die Startreihenfolge im CMOS-Setup-Programm und startete den Rechner neu.

Wichtig

In den CompTIA-Lernzielen wird eine *CD* als mögliches Installationsmedium aufgeführt, obwohl das seit Windows Vista, dem Vorgänger von Windows 7, nicht der Fall ist. Wenn das in der Prüfung vorkommt, sollten Sie die Frage sehr sorgfältig durchlesen.

Alternativ können Sie auch von Wechseldatenträgern starten, die über USB angeschlossen werden. Dazu gehören beispielsweise USB-Sticks, externe Festplatten und SSDs oder andere extern anschließ-

bare Laufwerke. Microsoft bietet sogar einen USB-Speicherstick als Installationsmedium an (Abbildung 11.11).



Abb. 11.11: USB-Speicherstick als Installationsmedium

Hinweis

Microsoft hat sich den Gegebenheiten angepasst. Die bevorzugte Methode zur Installation von Windows 10 sieht vor, eine ISO-Datei herunterzuladen und dieses ISO-Image auf ein startfähiges Medium zu schreiben. Mit dem *Windows Media Creation Tool*, das bei Microsoft zum Herunterladen bereitsteht, können Sie aus einem USB-Stick oder einer DVD leicht ein startfähiges Installationsmedium machen.

Sie möchten lieber kein Gerät am Rechner anschließen? Keine Sorge, Sie können auf die Installationsdateien auch via Netzwerk zugreifen. Mehr dazu im Abschnitt *Windows-Installation per Netzwerk* weiter hinten in diesem Kapitel.

Viele Hersteller richten auf der primären Festplatte eine kleine verborgene Partition ein, die ein Festplattenabbild einer fabrikneu installierten Windows-Version enthält. Wenn Ihre Windows-Installation nicht mehr funktioniert oder stark durcheinandergeraten ist, können Sie von dieser *Wiederherstellungspartition* oder *Recovery-Partition* starten und Windows neu installieren. Kapitel 16 (*Fehlerbehebung*) befasst sich ausführlicher mit der Recovery-Partition und verschiedenen anderen Wiederherstellungsmethoden.

Wichtig

In den Lernzielen der CompTIA A+-Prüfung 220-1002 ist davon die Rede, dass die »Interne Festplatte (Partition)« die Möglichkeit bietet, Windows zu installieren. Ich kann nur vermuten, dass damit die verborgene Recovery-Partition gemeint ist.

11.2.2 Installationsmethoden

Sie können Windows auf verschiedene Weise installieren. Bei einer *Neuinstallation* wird das Betriebssystem auf eine leere Festplatte aufgespielt oder ein bereits vorhandenes vollständig durch das neue Betriebssystem ersetzt. Bei einem *Upgrade* wird eine bereits vorhandene Version durch eine aktuellere ersetzt, wobei jedoch alle bestehenden Hardware- und Software-Einstellungen übernommen werden. Sie können auch mehrere Windows-Versionen auf einem Rechner installieren, wenn Sie eine *Multiboot-Installation* durchführen. Sehen wir uns die verschiedenen Optionen genauer an.

Neuinstallation

Bei einer *Neuinstallation* wird eine vorhandene Windows-Installation nicht beachtet. Auch bei einem neuen System mit noch leerer Festplatte wird eine Neuinstallation durchgeführt. Der Vorteil einer Neuinstallation besteht darin, dass Probleme des alten Betriebssystems nicht auf das neue übertragen werden. Der Nachteil besteht darin, dass Sie alle Anwendungen neu installieren und den Desktop und alle Anwendungen entsprechend den Vorlieben des Benutzers neu konfigurieren müssen. Für die Neuinstallation stellen Sie normalerweise das CMOS so ein, dass es erst von einer optischen Disc oder per USB und dann erst von der Festplatte oder SSD bootet. Anschließend starten Sie Windows von einem Installationslaufwerk. Während des Installationsvorgangs können Sie die Festplatte oder SSD partitionieren und formatieren.

Hinweis

In den Lernzielen der CompTIA A+-Prüfung 220-1002 werden PC AUFFRISCHEN und SYSTEMWIEDERHERSTELLUNG als Windows-Installationsmethoden erwähnt. In manchen Situationen ist das auch richtig. Sowohl PC AUFFRISCHEN als auch SYSTEMWIEDERHERSTELLUNG versuchen, das gesamte Betriebssystem oder einen Teil davon neu zu installieren, um ein nicht ordnungsgemäß funktionierendes System zu reparieren. Die SYSTEMWIEDERHERSTELLUNG sehen wir uns in Kapitel 14 genauer an und PC AUFFRISCHEN nehmen wir im Rahmen der Fehlerbehebung in Kapitel 16 in Angriff.

Upgrade-Installation

Wenn man in den Genuss einer neuen Betriebssystemversion kommen wollte, musste man jahrzehntelang die neue Version beschaffen (also in der Regel kaufen) und dann eine sogenannte Upgrade-Installation durchführen. So könnte es beispielsweise sein, dass Sie eine ältere Windows-Version auf Windows 10 upgraden möchten. Sehen wir uns also die Upgrade-Installation an.

Bei einem *Upgrade* wird das neue Betriebssystem in denselben Ordnern wie das alte bzw. in der Sprache der Techniker *über* das alte installiert. Das neue Betriebssystem ersetzt das alte, es bleiben aber alle gespeicherten Daten erhalten und alle persönlichen Einstellungen (Schriftarten, Desktop-Hintergrund usw.) werden übernommen. Sie müssen Ihre Lieblingsprogramme also nicht neu installieren! Abbildung 11.12 zeigt den Start einer Windows-Installation, und Sie werden gefragt, ob Sie ein Upgrade durchführen möchten.

Wichtig

Microsoft bezeichnet eine Upgrade-Installation oft als *direktes Upgrade*, daher wird der Begriff Ihnen in der Prüfung vielleicht begegnen. Allerdings verwendet Microsoft den Begriff auch für einen völlig anderen Vorgang (»Installation reparieren«). Achten Sie bei den Prüfungsfragen also genau auf den Kontext. *Installation reparieren* kommt in Kapitel 16 zur Sprache.



Abb. 11.12: Windows-Installation

Vor der Upgrade-Installation sollten Sie unbedingt *immer* ein Backup aller Benutzerdateien erstellen! Verwenden Sie die Bordmittel von Windows oder ein Programm eines Drittherstellers, aber überspringen Sie diesen Schritt nicht.

Um mit dem Windows-Upgrade zu beginnen, müssen Sie das entsprechende Programm von der optischen Disc oder dem USB-Laufwerk starten. Dazu legen Sie üblicherweise eine Windows-Installations-Disc ein, während Ihr altes Betriebssystem läuft, wodurch automatisch das Installationsprogramm startet. Sie werden dann gefragt, ob Sie ein Upgrade oder eine Neuinstallation durchführen möchten. Wenn Sie die Neuinstallation auswählen, wird das vorhandene Betriebssystem vor der Installation entfernt.

Hinweis

Vor dem Upgrade eines Betriebssystems müssen Sie alle laufenden Anwendungen schließen!

Multiboot-Installation

Bei einer dritten Option, die Sie kennen sollten, handelt es sich um die *Dual-Boot-* oder *Multiboot-Installation*. Das bedeutet, dass Ihr Rechner mehrere Windows-Versionen beherbergt. Beim Einschalten des Rechners werden Sie dann jeweils in einem Menü gefragt, welche Windows-Version Sie starten möchten (Abbildung 11.13).

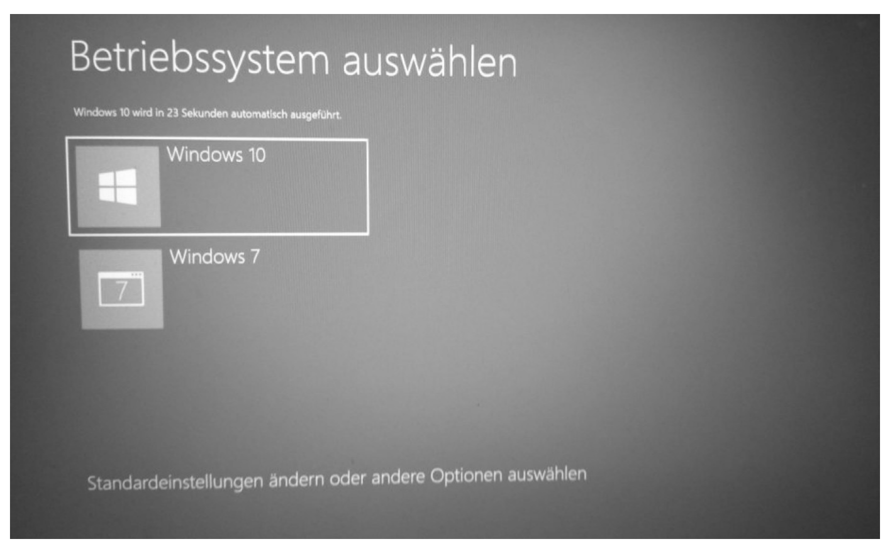


Abb. 11.13: Auswahl eines Betriebssystems nach einer Multiboot-Installation

Wie Sie aus Kapitel 9 wissen, erlaubt Windows es, die C:-Partition zu verkleinern. Wenn Sie also Dual-Boot einrichten möchten, aber nur über eine einzige Festplatte verfügen, können Sie dies tun, selbst wenn Windows bereits auf der C:-Partition installiert ist und die gesamte Festplatte belegt. Verkleinern Sie das Volume mit der Datenträgerverwaltung und richten Sie mit dem frei gewordenen Speicherplatz eine zusätzliche Partition ein, auf der Sie dann eine weitere Windows-Version installieren können.

Apple stellt ein exzellentes Tool namens *Boot Camp* zur Verfügung, das es Ihnen gestattet, Windows auf Apple-Rechnern zu installieren. Nachdem die Installation erledigt ist, können Sie dank Boot Camp beim Einschalten des Computers entscheiden, ob Sie macOS oder Windows starten möchten. Wenn Sie ein nur für Windows verfügbares Programm (Räusper ... Spiele?) benötigen, aber nur Apple-Rechner besitzen, dann ist Boot Camp das geeignete Werkzeug.

Mit Multiboot können Sie auch wahlweise Windows oder Linux starten. Bei der Installation von Linux wird die Fähigkeit, verschiedene Betriebssysteme zu starten, standardmäßig eingerichtet. Das gilt in umgekehrter Richtung aber nicht: Sie müssen *zuerst* Windows installieren, dann Linux.

Hinweis

Wenn Sie einen Rechner für Multiboot konfigurieren, müssen Sie zwei grundlegende Regeln berücksichtigen: Erstens muss die Systempartition mit einem Dateisystem formatiert sein, das von allen installierten Betriebssystemen unterstützt wird, und zweitens müssen Sie immer erst die älteren und dann die neueren Betriebssysteme installieren (bzw. zuerst Windows und dann andere Betriebssysteme wie Linux).

Weitere Installationsverfahren

Insbesondere wenn viele Rechner identisch konfiguriert werden müssen, werden in mittleren und größeren Unternehmen häufig anspruchsvollere Installationsverfahren eingesetzt. Oft werden dabei die Quelldateien in einem freigegebenen Ordner auf einem Netzwerkserver abgelegt. Wenn Techniker dann ein neues Betriebssystem installieren, muss der Rechner nur noch gestartet und mit dem entsprechenden Netzwerkordner verbunden werden, um die Installation von dort aus starten zu können. Man bezeichnet das als *Netzwerkinstallation* (Abbildung 11.14). Für dieses Verfahren gibt es viele Varianten und es lässt sich über spezielle Skripts automatisieren, die die gewünschten Optionen und Komponenten auswählen. Über diese Skripts lassen sich nach abgeschlossener Installation des Betriebssystems

auch benötigte Anwendungen installieren. Dabei sind nach dem Start der Installation keine weiteren Benutzereingriffe mehr erforderlich. Diese Art der Installation wird als *unbeaufsichtigte Installation* bezeichnet.

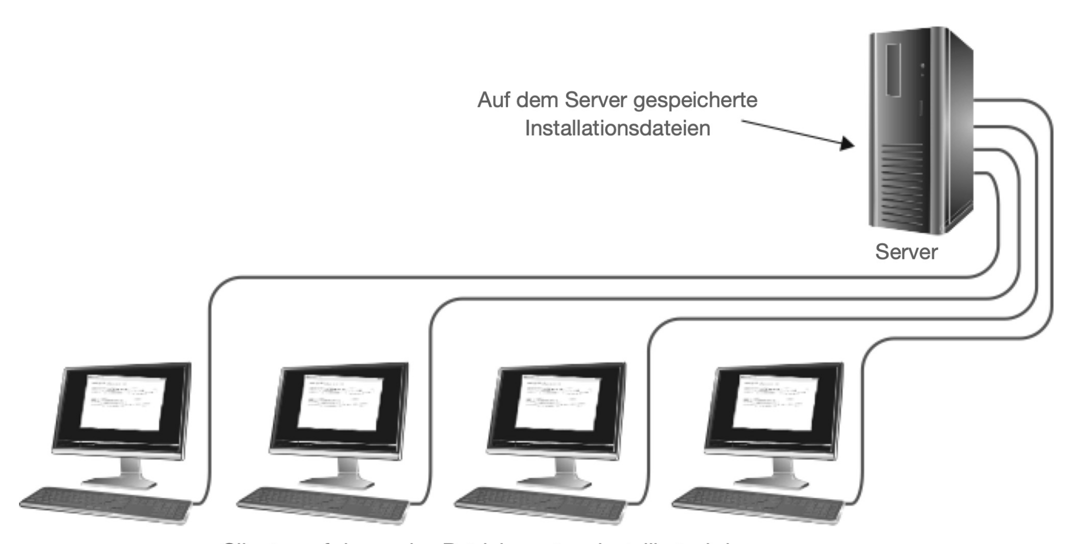


Abb. 11.14: Netzwerkinstallation

Eine weitere Möglichkeit zur wiederholten Installation standardisierter Konfigurationen bieten sogenannte *Image-Dateien*, die ein Abbild kompletter Festplatten enthalten, in denen sich das Betriebssystem und meist auch vorinstallierte Versionen aller benötigten Anwendungsprogramme befinden (Abbildung 11.15).

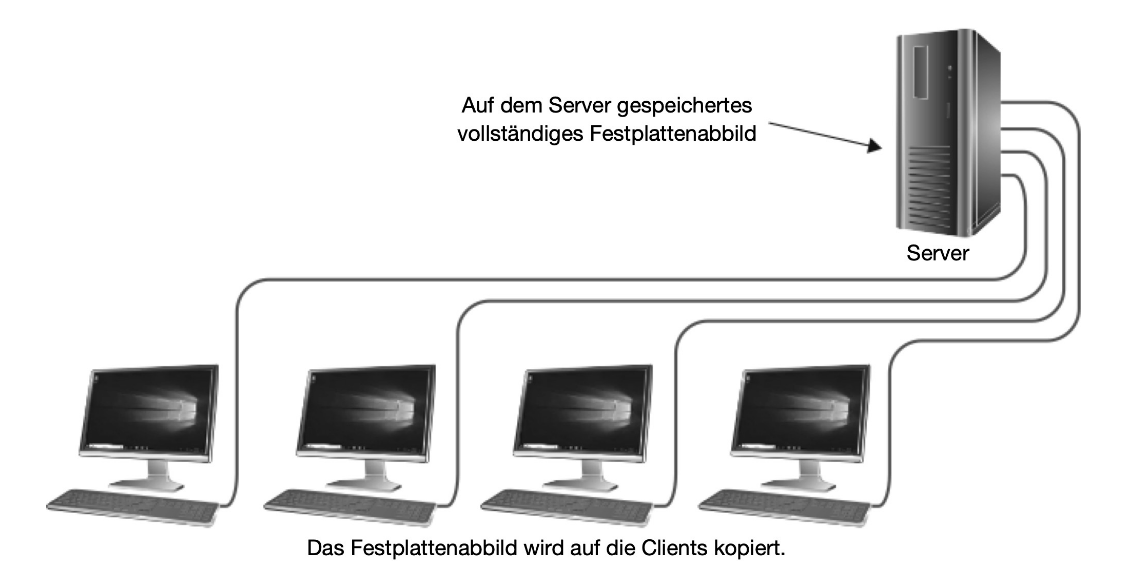


Abb. 11.15: Klonen des Festplattenabbilds über das Netzwerk

Diese Images können auf Servern, optischen Discs oder USB-Sticks gespeichert werden. Dann muss der Techniker nur noch spezielle Programme starten, mit denen die Image-Datei auf die lokale Festplatte oder SSD übertragen (»geklont«) wird. Auf diesem Gebiet war viele Jahre lang *Norton Ghost* von Symantec führend. Heutzutage bietet Symantec die *Symantec Ghost Solution Suite* an. *Clonezilla* und *True Image* (von Acronis) sind weitere Programme, die Ähnliches leisten.

Wichtig

Microsoft liefert zusammen mit Windows 10 ein Kommandozeilenprogramm namens *Deployment Image Servicing and Management* (`dism.exe`) aus (das bislang in der CompTIA A+-Prüfung aber nicht ausführlich vorkommt), um das Klonen von Festplattenabbildern zu ermöglichen. Besuchen Sie die TechNet-Website oder sehen Sie in der Hilfe der PowerShell nach, um weitere Informationen zu erhalten. dism könnte Teil der CompTIA A+-Prüfung sein.

11.2.3 Der Installations- und Aktualisierungsvorgang

Grundsätzlich führt man bei der Installation aller Betriebssysteme eine Reihe mehr oder weniger einheitlicher Schritte durch. Sie schalten den Computer ein, legen ein Installationsmedium ins optische Laufwerk, schließen ein USB-Laufwerk an, oder greifen anderweitig auf die Installationsdateien zu, folgen den Anweisungen des Installationsassistenten und warten, bis alles erledigt ist. Zwischendurch müssen Sie die *Lizenzbedingungen* (*EULA – End User License Agreement*) akzeptieren und geben den Product Key ein, der belegt, dass Sie kein Pirat sind. Er ist zumeist auf der Hülle der Installations-Disc oder der Verpackung des USB-Speichersticks angegeben. Aber der Teufel steckt hier in den Details!

Erstens sind in den CompTIA-Lernzielen die folgenden Betriebssystemversionen aufgeführt: Windows 7, Windows 8, Windows 8.1 und Windows 10. Ich gehe davon aus, dass die CompTIA nur an Upgrade-Installationen älterer Windows-Versionen auf Windows 10 interessiert ist. Wenn Sie eine Upgrade Installation von Windows 7 auf Windows 8.1 durchführen möchten ... Viel Glück!

Zweitens müssen Sie sich für eine Neuinstallation, eine Upgrade-Installation oder eine Multiboot-Installation entscheiden. Sehen Sie sich die vorhin beschriebenen Schritte noch einmal an, um eine Entscheidung zu fällen. Im Folgenden ist eine Neuinstallation beschrieben.

Drittens ist Windows nicht das einzige Betriebssystem, das es gibt. Auch wenn im folgenden Beispiel Windows verwendet wird, sollten Sie bedenken, dass bei der Installation von macOS und allen Linux-Distributionen ähnliche Schritte erforderlich sind.

Neuinstallation von Windows

Sie müssen Ihren Rechner zunächst von irgendeinem Windows-Installationsmedium starten. Wenn nach dem Booten das Installationsprogramm gestartet wurde, müssen Sie zunächst angeben, ob Sie ein 32-Bit- oder ein 64-Bit-Windows installieren möchten. Da fast alle CPUs 64 Bit unterstützen, sollten Sie die letztere Option auswählen (Abbildung 11.16). Sollte das nicht möglich sein: Keine Sorge, die Installation wird fehlschlagen und Sie können es erneut versuchen.

Wichtig

Wenn Sie Windows auf Laufwerken installieren, die über einen RAID-Controller angeschlossen sind, werden Sie am Anfang des Installationsvorgangs aufgefordert, F6 zu drücken, um gegebenenfalls erforderliche Treiber eines Drittherstellers zu laden. Wenn Sie dieser Aufforderung Folge leisten, passiert zunächst nichts weiter. Sie werden später aufgefordert, eine Disc mit Treibern einzulegen.

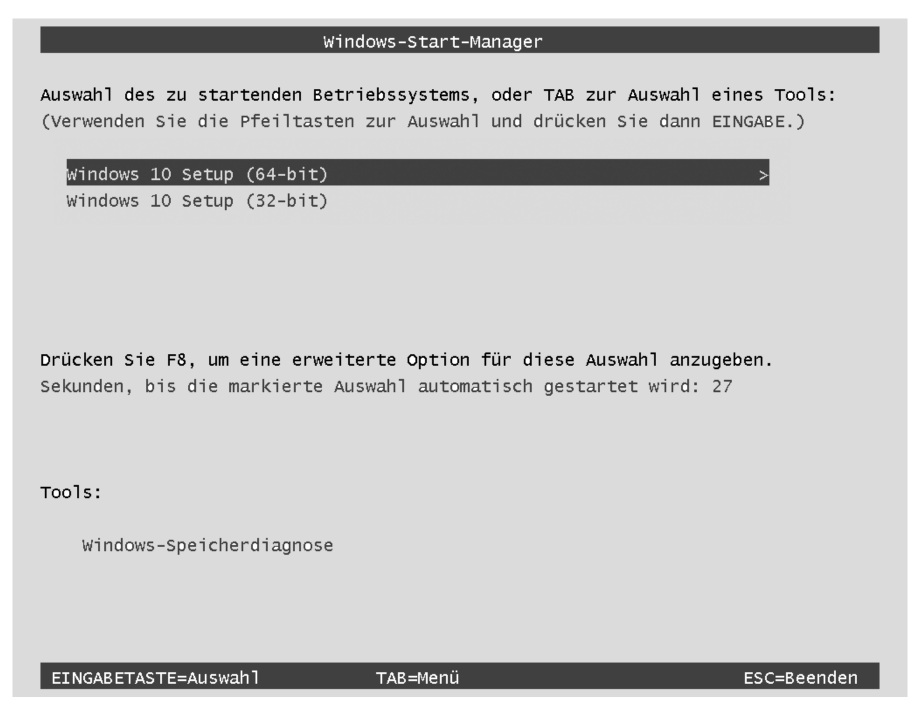


Abb. 11.16: Auswahl von 32 oder 64 Bit

Anschließend wird ein Bildschirm angezeigt, in dem Sie Ihre Sprache, Uhrzeit- und Währungsformat sowie Tastatureinstellungen festlegen können (Abbildung 11.17). Klicken Sie auf WEITER, um fortzufahren.



Abb. 11.17: Regionale Einstellungen von Windows

Auf dem nächsten Bildschirm wird der Installationsvorgang gestartet, aber beachten Sie die untere linke Ecke. Hier können Techniker die Reparaturprogramme der Installations-Disc starten (Abbildung 11.18). Mehr über diese Werkzeuge erfahren Sie in Kapitel 16. An dieser Stelle müssen Sie nur wissen, dass Sie diese durch Anklicken von COMPUTERREPARATUROPTIONEN starten können. Da es in diesem Kapitel nur um die Installation von Windows geht, klicken Sie JETZT INSTALLIEREN an.

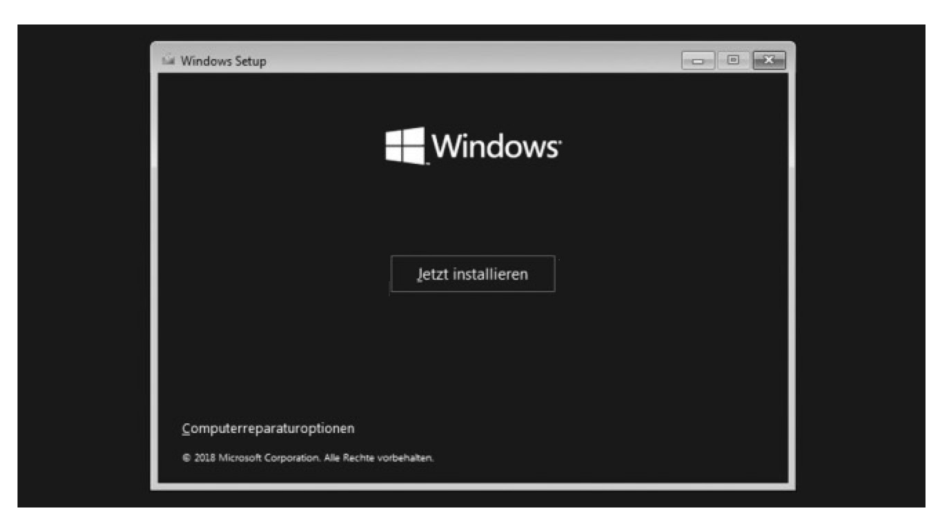


Abb. 11.18: Der Begrüßungsbildschirm bei der Installation von Windows

Auf dem nächsten Bildschirm werden Sie aufgefordert, den Product Key einzugeben, bevor Sie fortfahren können (Abbildung 11.19). Der Product Key liegt den Installationsmedien bei – verwahren Sie ihn sorgsam.

Alle Installationsmedien enthalten alle erhältlichen Editionen. Der Product Key bestätigt nicht nur den legalen Erwerb, sondern teilt dem Installationsprogramm auch mit, welche Edition Sie erworben haben.



Abb. 11.19: Der Bildschirm zur Eingabe des Product Keys

Wenn Sie auf ICH HABE KEINEN PRODUCT KEY klicken (oder vor Windows 10 das Feld zur Eingabe des Produktschlüssels leer lassen und die Schaltfläche WEITER anklicken), dann wird Ihnen ein Dialogfeld angezeigt, in dem Sie gefragt werden, welche Windows-Version Sie installieren wollen (Abbildung 11.20). Sie sollten nun aber nicht glauben, dass Sie damit eine Möglichkeit gefunden haben, Windows zu installieren, ohne dafür zu bezahlen. Auf diesem Weg installieren Sie einfach nur eine 30-Tage-Testversion des Betriebssystems. Nach 30 Tagen können Sie nicht mehr bis zum Desktop durchstarten, ohne einen gültigen Produktschlüssel eingegeben zu haben, der zu der installierten Windows-Edition passt. Nach der Eingabe des Produktschlüssels werden Microsofts *Lizenzbedingungen* (*EULA – End User License Agreement*) angezeigt (Abbildung 11.21).

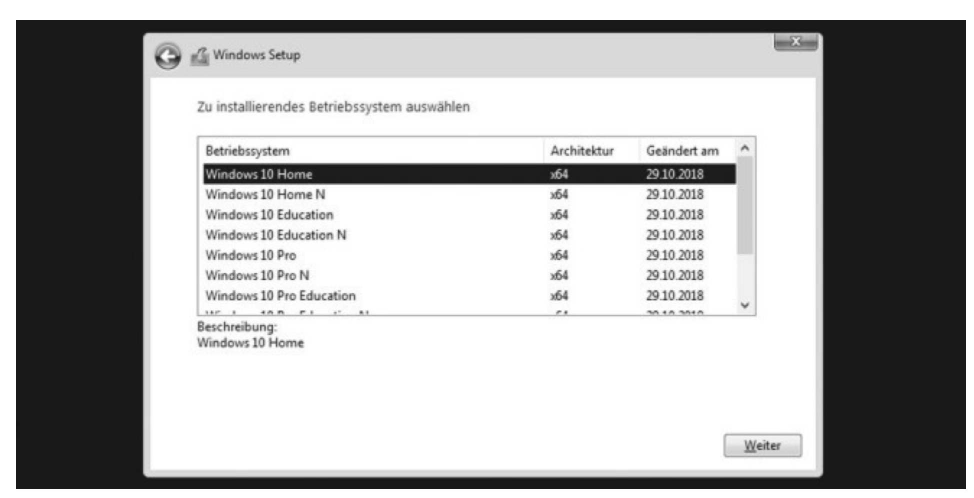


Abb. 11.20: Auswahl der zu installierenden Windows-Version

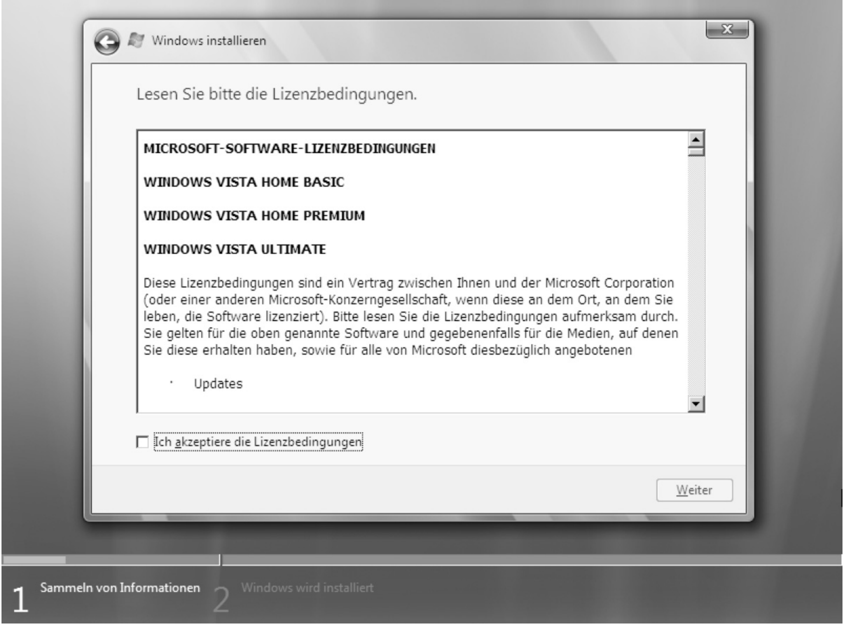


Abb. 11.21: Die Windows-EULA

Auf der nächsten Seite müssen Sie entscheiden, ob Sie ein Upgrade oder eine Neuinstallation durchführen wollen. Windows bezeichnet die Neuinstallation als benutzerdefiniert, wie Sie Abbildung 11.22 entnehmen können. Um eine Neuinstallation von Windows vorzunehmen und Partitionen zu bearbeiten, wählen Sie die Option BENUTZERDEFINIERT (ERWEITERT).



Abb. 11.22: Wählen Sie die Art der Installation.

Auf dem nächsten Bildschirm (Abbildung 11.23) können Sie Ihre Festplatten partitionieren und auswählen, in welcher Partition Windows installiert werden soll. Wenn Sie im Dialogfeld NEU oder in älteren Windows-Versionen LAUFWERKOPTIONEN (ERWEITERT) anklicken, wird Ihnen eine Reihe von Partitionierungsoptionen angezeigt (Abbildung 11.23).

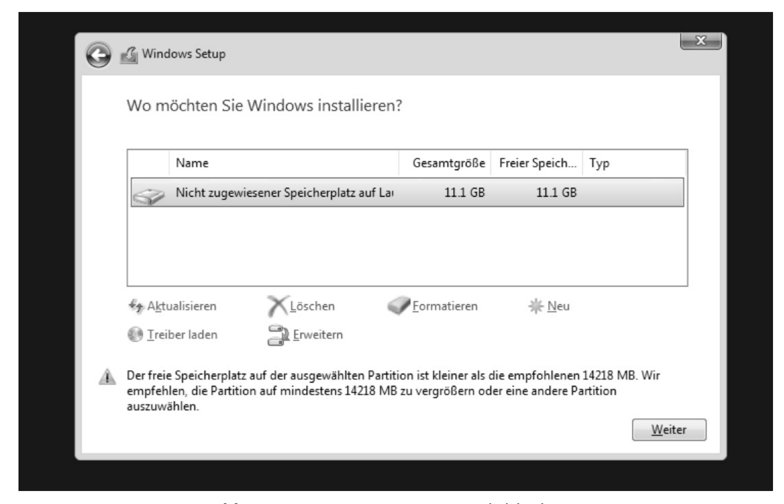


Abb. 11.23: Der Partitionierungsbildschirm

Wenn Sie Ihre Laufwerke partitioniert und eine Partition für die Windows-Installation ausgewählt haben, dann übernimmt das Installationsprogramm die Kontrolle und kopiert Dateien, entkomprimiert sie, installiert Funktionen und erledigt eine Menge der bei Rechnern üblichen Dinge. Das kann eine Weile dauern, also nutzen Sie die Gelegenheit, um einen Happen zu essen oder um *Krieg und Frieden* zu lesen.

Hinweis

So lange dauert die Windows-Installation nun auch wieder nicht. Das Einspielen von Windows 10 geht erheblich flotter vonstatten als bei vorhergehenden Versionen – insbesondere auf einer SSD.

Wenn Windows das Entpacken und die eigene Installation abgeschlossen hat, bietet die Sprachassistentin Cortana ihre Hilfe an. Abbildung 11.24 zeigt, wo Sie konfigurieren, ob das System zur persönlichen Verwendung dient oder in einer Organisation zum Einsatz kommt. Beachten Sie, das letztere Option den Computer *nicht* zu einer Active-Directory-Domäne hinzufügt, sie erweist sich aber als nützlich, wenn ein Unternehmen Abonnementsdienste wie Microsoft Office 365 verwendet.



Abb. 11.24: Auswahl zwischen persönlicher Verwendung und Einrichtung für eine Organisation

Auf dem nächsten Bildschirm werden Sie zur Eingabe eines Benutzernamens und eines Kennworts für das Konto des Hauptbenutzers aufgefordert (Abbildung 11.25). Das Anlegen dieses Kontos ist bei allen Betriebssystemen erforderlich. Cortana fordert Sie auf, einen Namen auszuwählen, und möchte Sie dazu bewegen, ein Microsoft-Konto anzulegen, falls Sie noch nicht über ein solches verfügen. Ich überspringe das Anlegen dieses Kontos und erstelle ein reguläres lokales Benutzerkonto. Meine Redakteure verwenden Microsoft-Konten. Was für Sie am besten geeignet ist, müssen Sie selbst entscheiden.



Abb. 11.25: Angabe eines Benutzernamens

Microsoft und Apple sind sehr darauf bedacht, dass sich Benutzer mit einem Konto anmelden, das nicht mit dem PC, sondern mit Microsoft bzw. Apple verknüpft ist. Solche Konten bieten eine gewisse Bequemlichkeit und sind für Privatleute akzeptabel, aber Organisationen, die größer sind als ein Tante-Emma-Laden, werden auf diese Konten verzichten und die herkömmlichen Konten verwenden. Ich empfehle Ihnen das ebenfalls.

Wichtig

Rechnen Sie damit, dass in der CompTIA A+-Prüfung Fragen vorkommen, die sich auf die Installation von Desktop-Computern beziehen, insbesondere auf die Einrichtung von Benutzerkonten. Hier stehen bei aktuellen Geräten vier Möglichkeiten zur Auswahl: lokales Benutzerkonto, globales Konto, Organisationskonto und Domänenkonto.

Microsoft hat an dieser Stelle eine weitere Konfigurationsmöglichkeit hinzugefügt, nämlich Einstellungen zum Datenschutz (Abbildung 11.26). Aber selbst dann, wenn Sie hier alles deaktivieren, verhindert das nicht, dass Microsoft einige Informationen erhält.

Hinweis

Wenn Sie diesen Bildschirm hinter sich gelassen haben, beginnt die eigentliche Windows-Installation (Abbildung 11.27) und Sie werden gewarnt, dass es ein Weilchen dauern kann. Sind Sie nicht auch der Ansicht, dass das für eine Software doch einigermaßen höflich ist?

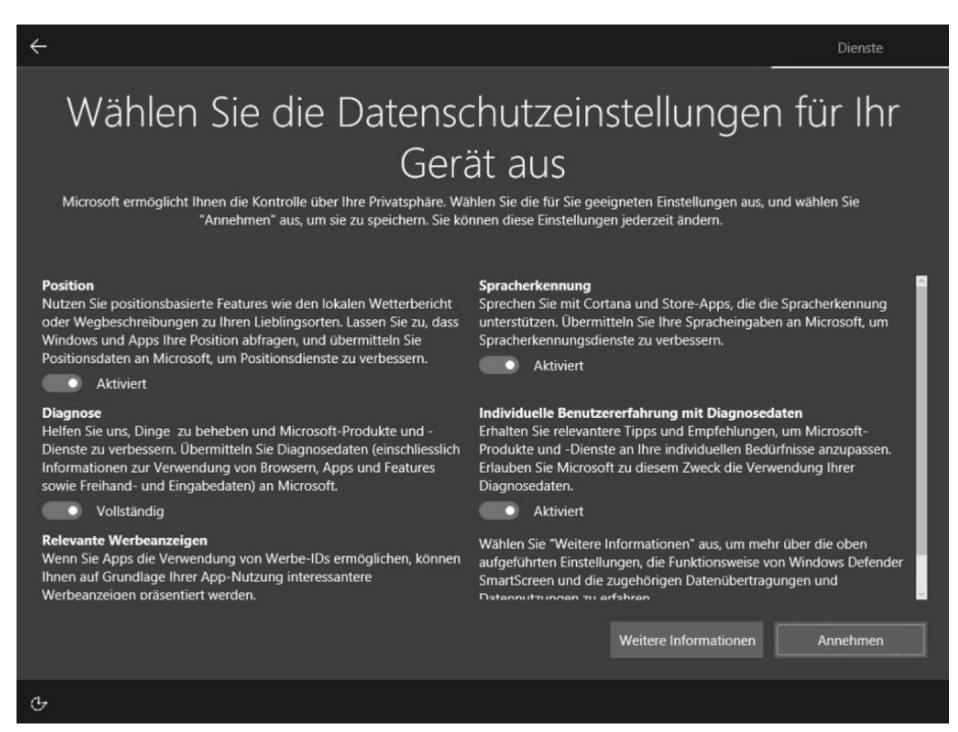


Abb. 11.26: Einstellungen zum Datenschutz



Abb. 11.27: Danke für den Hinweis!

Windows-Installation per Netzwerk

In manchen Fällen müssen Techniker in größeren Unternehmen Windows sehr häufig installieren. Wenn Sie sich um 100 PCs kümmern müssen und Microsoft eine neue Windows-Version veröffentlicht, möchten Sie sicher nicht mit einer Installations-DVD von Büro zu Büro laufen und eine Installation nach der anderen durchführen. Automatisierte (unbeaufsichtigte) Installationen haben Sie bereits kennengelernt, Netzwerkinstallation gehen jedoch noch einen Schritt weiter.

Oder stellen Sie sich eine andere Situation vor. Sie sind noch immer Techniker in einem großen Unternehmen, und Ihr Chef hat beschlossen, dass alle PCs ein Image mit einer festgelegten Auswahl

an Programmen und vorgegebener Konfiguration verwenden sollen. Das Image muss auf sämtliche Rechner übertragen werden, von denen die meisten jedoch kein optisches Laufwerk besitzen. Da kommt die Installation per Netzwerk wie gerufen!

Der Begriff »Netzwerkinstallation« kann eine Reihe verschiedener Werkzeuge umfassen, je nachdem, welche Windows-Version Sie verwenden. Entscheidend ist, dass die Geräte, auf denen das Betriebssystem installiert werden soll (die Clients), über das Netzwerk mit einem Server verbunden sind. Auf dem Server könnte Windows 7, 8, 8.1 oder 10 laufen, vielleicht handelt es sich aber auch um einen ausgewachsenen Windows-Server. Jedenfalls muss der Server ein Image bereitstellen, das entweder eine Standardinstallation von Windows enthält, oder eine vom Netzwerkadministrator erstellte angepasste Version.

Die Verwaltung des Servers ist Aufgabe eines Netzwerkadministrators. Die Einrichtung eines solchen Servers, der Windows-Installationen und Images bereitstellt, geht über die Anforderungen der CompTIA A+-Prüfung hinaus.

Auf den Clients kommt bei Netzwerkinstallationen *PXE* (*Preboot Execution Environment*) zum Einsatz. PXE verwendet verschiedene Protokolle wie IP, DHCP und DNS, um Ihrem Computer das Booten per Netzwerk zu ermöglichen. Installationsmedien oder USB-Speicherstick sind nicht erforderlich. Schließen Sie Ihren Computer einfach nur ans Netzwerk an und ab geht's! Nun gut, *etwas* komplizierter ist die Sache schon.

Zum Aktivieren von PXE müssen Sie sich ins BIOS-Setup begeben. Suchen Sie den Bildschirm, auf dem die Netzwerkkarten konfiguriert werden (Abbildung 11.28). Wenn es dort eine PXE-Einstellung gibt, aktivieren Sie diese. Außerdem müssen Sie die Startreihenfolge ändern, damit der PC als Erstes einen Start über das Netzwerk versucht.

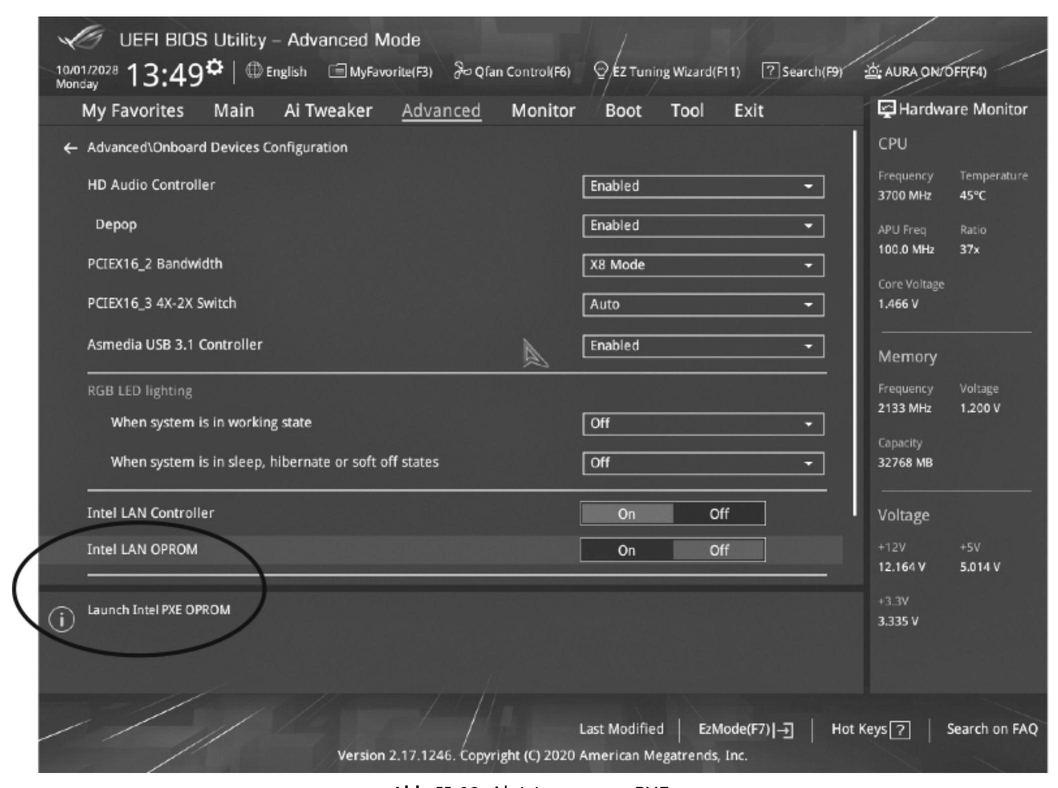


Abb. 11.28: Aktivierung von PXE

Hinweis

Die meisten Netzwerkkarten unterstützen PXE, aber nicht alle. Wenn Sie ohne PXE über das Netzwerk booten möchten, können Sie ein Startlaufwerk erstellen, das den PC zwingt, über das Netzwerk zu booten.

Nach dem Neustart des Rechners sehen Sie anfangs den üblichen Startbildschirm. Dann sollte jedoch eine Anweisung wie PRESS F12 FOR NETWORK BOOT erscheinen (es ist fast immer F12). Der PC sucht nun im Netzwerk nach einem Server, mit dem er sich verbinden kann. Gelingt das, werden Sie erneut aufgefordert, F12 zu drücken, um den Startvorgang über das Netzwerk fortzusetzen (Abbildung 11.29).

```
Network boot from Intel E1000
Copyright (C) 2003-2008  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 D7 9B 6B  GUID: 564DCC2E-04EA-ACE1-381B-5148E8D79B6B
CLIENT IP: 10.12.14.51  MASK: 255.0.0.0  DHCP IP: 10.12.14.10
GATEWAY IP: 10.12.14.1

Downloaded WDSNBP...

Press F12 for network service boot
_
```

Abb. 11.29: Start über das Netzwerk

Abhängig von der Anzahl der Images, die der Server bereithält, gelangen Sie unmittelbar zum Startbildschirm der Windows-Installation oder werden aufgefordert, eins von mehreren Images auszuwählen. Wenn Sie Ihre Wahl getroffen haben, sollte alles Weitere wie bei einer Windows-Installation von einem lokalen optischen Laufwerk verlaufen.

macOS per Netzwerk installieren

NetBoot ist Apples Werkzeug für diese Aufgabe und gestattet es, macOS auf verschiedene Weisen über das Netzwerk zu installieren. So können Sie beispielsweise via NetBoot mehrere identische Rechner mit macOS von einem Server starten – die Geräte sind dann so konfiguriert, wie Sie es wünschen. Alle von einem Benutzer vorgenommenen Änderungen sind wieder verschwunden, sobald sie den Rechner neu starten. Für die Nutzung in Schulklassen oder auf Konferenzen ist das äußerst praktisch.

Eine andere Möglichkeit besteht darin, ein und dasselbe Betriebssystem-Image auf den lokalen Festplatten mehrerer entfernter Rechner zu installieren. Auf diese Weise können Sie unternehmensweite Aktualisierungen vornehmen, z.B. wenn es eine neue Standardkonfiguration gibt.

Und schließlich können Sie NetBoot auch dazu verwenden, einzelne Programme »in einem Rutsch« auf vielen Computern zu installieren. Zum Verteilen neuer Programmversionen in größeren Organisationen ist das ideal.

11.2.4 Behebung von Installationsproblemen

Der Begriff »Installationsproblem« ist eigentlich irreführend, denn der Installationsprozess selbst schlägt fast nie fehl. Normalerweise gibt es andere Gründe während der Installation, die zu deren

Abbruch führen. Schauen Sie sich im Folgenden einige typische Installationsfehler und deren Behebung an.

Defekte Installationsmedien

Falls Sie wirklich Probleme bei der Windows-Installation bekommen, dann sind hoffentlich nur defekte Installationsmedien der Grund dafür, wie etwa eine verkratzte DVD oder ein defektes USB-Laufwerk. Es ist immer besser, wenn Fehler ganz am Anfang und nicht erst mitten in der Installation oder kurz vor ihrem Ende auftreten.

RAID-Verbund nicht gefunden Wenn während der Windows-Installation ein RAID-Verbund nicht gefunden wird, könnte das daran liegen, dass der passende Treiber für das RAID-Laufwerk oder den RAID-Controller fehlt. Wenn die Festplatten in der Konfigurationssoftware des RAID-Controllers angezeigt werden, handelt es sich fast mit Sicherheit um ein Treiberproblem. Besorgen Sie sich den Treiber vom Hersteller und starten Sie die Installation erneut. Drücken Sie dann ganz am Anfang des Installationsvorgangs F6, wenn Sie dazu aufgefordert werden. Wenn Sie F6 drücken, scheint zunächst nichts zu passieren, Sie werden später jedoch zur Treiberinstallation aufgefordert.

Beim Booten vom Startdatenträger wird kein Bootgerät gefunden Entweder ist in diesem Fall der Datenträger im Startlaufwerk defekt oder das Startlaufwerk wurde im CMOS-Setup nicht richtig festgelegt. Ändern Sie das Startlaufwerk wie in Kapitel 5, *BIOS und CMOS*, beschrieben.

Fehler im Grafikmodus

Sobald der Grafikmodus der Installation erreicht ist, können Fehler zahlreiche Ursachen haben, wie etwa Probleme mit der Hardware oder mit Treibern. Fehler bei der Hardware-Erkennung lassen sich bei allen Setup-Versionen durch vorherige Prüfung der Kompatibilität vermeiden. Wenn Sie diesen vorbereitenden Schritt übersprungen haben, dann haben Sie vielleicht Glück und es sind nur unkritische Komponenten betroffen. Dann können Sie das Problem später beheben. Wenn Sie Ihre Hausaufgaben vorher nicht gemacht haben, dann müssen Sie nach der Windows-Installation nach kompatiblen Treibern suchen.

Jede Windows-Installation ist darauf angewiesen, dass das Setup-Programm den Computertyp (insbesondere Mainboard und BIOS) korrekt erkennt und die richtige Hardwareunterstützung installiert. Microsoft hat Windows so entwickelt, dass es unterschiedliche Hardwareplattformen unterstützt, und verwendet als Unterbau speziell auf Hardware zugeschnittene Software, die *Hardwareabstraktionsebene* (*HAL – Hardware Abstraction Layer*) genannt wird.

Systemabstürze während der Installation

Systemabstürze sind eines der schwierigsten Probleme, die während einer Installation auftreten können, weil sie einem keinen Hinweis auf die Problemursache geben. Nachfolgend einige Dinge, die Sie prüfen können, wenn ein System während der Installation abstürzt.

Disc, Laufwerk oder Image-Datei beschädigt Auch optische Discs, optische oder Festplattenlaufwerke mit Defekten können Systemabstürze verursachen. Ebenso kann eine beschädigte Image-Datei auf einem USB-Stick oder eine defekte heruntergeladene ISO-Datei die Installation aus der Bahn werfen. Prüfen Sie, ob die Discs verkratzt oder verunreinigt sind, und säubern oder ersetzen Sie diese. Legen Sie eine Disc in das Laufwerk ein, von der Sie wissen, dass sie in Ordnung ist. Wenn derselbe Fehler erneut auftritt, müssen Sie das Laufwerk oder möglicherweise die ISO-Datei ersetzen.

Protokolldateien Windows-Versionen vor Windows 10 erzeugen eine Reihe spezieller Textdateien, die *Protokolldateien* genannt werden und in denen der Fortschritt bestimmter Vorgänge aufgezeichnet wird. Windows erstellt eine Reihe verschiedener Protokolldateien für unterschiedliche Zwecke. Der Installationsvorgang erzeugt rund 20 verschiedene Protokolldateien, die entsprechend der jeweiligen Installationsphase angelegt werden. Allerdings wird in jeder Phase eine Datei namens `setuperr.log` erzeugt, um die Fehler dieser Installationsphase aufzuzeichnen. Windows 10 erzeugt

(unter anderem) im Verzeichnis `%WINDIR/anther` die Datei `setup.etl`, die Sie mit der Ereignisanzeige öffnen können.

Diese Dateien werden im Windows-Verzeichnis (dort, wo das Betriebssystem installiert ist) abgelegt. Da die Betriebssysteme leistungsfähigere Wiederherstellungsoptionen bereitstellen, ist es allerdings ziemlich unwahrscheinlich, dass Sie eine solche Log-Datei jemals lesen und anhand der darin enthaltenen Informationen etwas reparieren werden! Die Protokolldateien sind aber praktisch, wenn Sie Microsoft oder einen Hardwarehersteller anrufen, denn dort gibt es Leute, die den Inhalt dieser Dateien wirklich verstehen! Machen Sie sich wegen der Protokolldateien keine Gedanken hinsichtlich der CompTIA A+-Prüfung. Sie sollten lediglich die Namen der Dateien und ihren Speicherort kennen. Die Details können Sie den wahren Freaks überlassen.

Tipp: Speicherort der Protokolldateien

1. Besuchen Sie die Webseite `https://technet.microsoft.com/de-de/library/hh824819.aspx`, wenn Sie eine andere Version als Windows 10 verwenden, und sonst `https://docs.microsoft.com/de-de/windows-hardware/manufacture/desktop/windows-setup-log-files-and-event-logs`.
2. Sehen Sie sich die Speicherorte und die Beschreibung der Protokolldateien an.
3. Navigieren Sie mit dem Explorer auf Ihrem eigenen PC zu den genannten Speicherorten und suchen Sie nach den Protokolldateien.

Wer weiß, ob Sie nicht auf dem besten Weg sind, ein Protokollleser zu werden!

Wichtig

Rechnen Sie in den CompTIA-Prüfungen 1001 und 1002 mit Fragen zu den während eines Upgrades erstellten Protokolldateien. In der Prüfung 1002 könnte es Fragen zu der Situation geben, dass sich Windows an veralteten Treibern oder fehlerhaften Netzwerkeinstellungen »verschluckt« und nicht startet. Anhand der Protokolldateien lassen sich solche Fehler schnell finden, die Sie dann beheben können, bevor Sie versuchen, ein Upgrade auf Windows 10 auszuführen.

In der Prüfung 1001 könnte es Fragen zur Hardware geben, insbesondere zur Konfiguration im System-Setup. Das CompTIA-Lernziel 5.3 nennt Protokolleinträge und Fehlermeldungen bei Problemen mit grundlegender Hardware, wie dem Mainboard oder dem RAM. Wenn Sie in der Protokolldatei einen derartigen Fehler finden, sollten Sie versuchen, die Standardeinstellungen zu verwenden. Das hat in vielen Fällen funktioniert.

11.3 Aufgaben nach der Installation

Sie denken vielleicht, das reicht für einen Arbeitstag, aber noch sind einige Dinge zu erledigen. Dazu gehören die Aktualisierung des Betriebssystems selbst, das Einspielen von Patches und Service Packs, Treiberaktualisierungen, gegebenenfalls die Wiederherstellung von Datendateien des Benutzers und möglicherweise das Migrieren oder Ausrangieren von Systemen.

11.3.1 Patches, Service Packs und Aktualisierungen

Jemand hat einmal von einem Flugzeug gesagt, dass es sich dabei um Millionen von Einzelteilen handelt, die in geschlossener Formation durch die Luft fliegen. Diese Analogie lässt sich auch ganz gut auf Betriebssysteme übertragen. Wir können sie sogar noch etwas weiter treiben, wenn Sie an all die Wartungsarbeiten denken, die notwendig sind, damit ein Flugzeug sicher fliegen kann. Wie beim Flugzeug wurden auch die Einzelteile (der Programmcode) des Betriebssystems von unterschiedlichen Personen und teilweise sogar extern entwickelt und hergestellt. Auch wenn alle Komponenten einzeln und das Betriebssystem insgesamt sorgfältig getestet wurden, lassen sich nicht alle möglichen Kombinationen

von Ereignissen testen. Manchmal sind Dinge einfach fehlerhaft. Programme zur Behebung derartiger Probleme werden *Patch* genannt.

Früher hat Microsoft Patches für einzelne Probleme veröffentlicht. Zudem wurden diese gesammelt, bis sie eine Art »kritische Masse« erreicht hatten und dann zu einem sogenannten *Service Pack* zusammengefasst. Windows 7 ist jedoch die letzte Version, für die Microsoft ein Service Pack bereitstellt. Heutzutage erhält Windows einzelne Aktualisierungen über das Internet.

Unmittelbar nach der Installation von Windows sollten Sie die neuesten Updates auf dem Rechner installieren. Das erfolgt am einfachsten, indem Sie Windows Update verwenden. Mehr darüber erfahren Sie in Kapitel 14, *Wartung und Optimierung*.

11.3.2 Treiber aktualisieren

Selbst wenn Sie Ihre Hausaufgaben erledigt haben, können Sie sich später dazu entschließen, anstelle der mit Windows gelieferten Standardtreiber aktuellere Treiber zu benutzen. Diese Strategie ist tatsächlich zu empfehlen, da die Installation eine ohnehin komplexe Aufgabe ist, die Sie sich dadurch erleichtern können, dass zunächst ältere und erprobte Treiber verwendet werden. Die aktuellen Treiber sind möglicherweise noch keine Woche alt. Wenn Sie diese erst nach Abschluss der Windows-Installation auf den Rechner übertragen, dann können Sie immer noch zu einem immerhin geeigneten Treiber zurückkehren, wenn sich herausstellt, dass der neue Treiber fehlerhaft ist.

11.3.3 Wiederherstellen von Datendateien (falls erforderlich)

Können Sie sich noch daran erinnern, dass Sie die Datendateien vor der Installation gesichert haben? Nicht? Dann sehen Sie noch einmal nach, denn jetzt ist es an der Zeit, diese wiederherzustellen. Wie Sie dabei vorgehen müssen, hängt vorwiegend von dem bei der Sicherung verwendeten Verfahren ab. Wenn Sie Programme von Drittanbietern verwendet haben, dann müssen Sie diese erst einmal installieren. Wenn Sie SICHERN UND WIEDERHERSTELLEN verwendet haben, dann haben Sie Glück, denn diese werden standardmäßig installiert. Wenn Sie die Daten einfach nur auf optische Discs, USB-Sticks, externe Laufwerke oder freigegebene Ordner im Netzwerk kopiert haben, dann kopieren Sie die Daten einfach zurück auf die lokale Festplatte. Gutes Gelingen!

11.3.4 Installation wichtiger Software

Der letzte Schritt ist die Installation der Software, die dafür sorgt, dass der Computer so funktioniert, wie sich Ihre Anwender das wünschen. Wenn Sie Software installieren, die eine Lizenz erfordert, müssen Sie diese zur Hand haben. Wenn Sie abonnierte Software installieren, wie Microsoft Office 365, benötigen Sie die passenden Benutzernamen und Kennwörter. Und vergessen Sie nicht, Steam zu installieren und ein paar vergnügliche Anwendungen herunterzuladen!

Wichtig

Rechnen Sie damit, dass in der Prüfung Fragen zu den letzten Schritten der Installation vorkommen: Installation von Treibern und Software sowie die Aktualisierung von Windows.

11.3.5 Umzug und Ausmusterung

Die Zeiten ändern sich und auch der Computermarkt befindet sich in ständigem Wandel. Irgendwann müssen Sie alte Systeme ausmustern. Das bedeutet, Sie müssen die Daten und Benutzer auf ein neues System übertragen (*Migration*), oder zumindest auf eine neue Festplatte, und dann das alte System sicher entsorgen. Microsoft stellt für diesen Zweck einige Werkzeuge zur Verfügung, und da Sie diese für die CompTIA A+-Prüfungen (und den nächsten neuen Rechner) kennen müssen, werde ich sie nachfolgend vorstellen.

Migrationstool für den Benutzerstatus (User State Migration Tool)

Wenn Sie einer der Computerbenutzer sind, die maximale Funktionalität und Leistung von ihrem Betriebssystem erwarten, dann werden Sie wahrscheinlich das *Migrationstool für den Benutzerstatus* (*USMT – User State Migration Tool*) nutzen wollen. USMT wird vorwiegend im Unternehmensumfeld genutzt, weil es in einer Windows-Server-Domäne ausgeführt werden muss. Wenn viele Benutzer auf neue Rechner umziehen müssen, dann ist USMT das geeignete Werkzeug. Wenn nur einige wenige Benutzer auf einen neuen Rechner umziehen müssen, dann verwenden Sie sinnvollerweise das nachfolgend beschriebene Windows-EasyTransfer.

Hinweis

Bei der Installation von Windows-Systemen im großen Stil ist USMT besonders praktisch. Microsoft stellt einen ausführlichen Überblick zur Verfügung, der die Vorteile und Grenzen von USMT beschreibt. Sie finden diese Informationen unter `https://docs.microsoft.com/de-de/windows/deployment/usmt/usmt-overview`.

Windows-EasyTransfer

Windows-EasyTransfer gestattet es Ihnen, Benutzerdaten und persönliche Einstellungen schnell und einfach zu migrieren. Unter Windows 7 finden Sie Windows-EasyTransfer im PROGRAMME-Menü unterhalb von ZUBEHÖR im Ordner SYSTEMPROGRAMME. Begeben Sie sich unter Windows 8/8.1 zum Startbildschirm, tippen Sie `EasyTransfer` und wählen Sie aus den Ergebnissen Windows-EasyTransfer aus. Unter Windows 10 ist das Programm leider nicht verfügbar.

Auf der ersten Seite von Windows-EasyTransfer erhalten Sie einfach ein paar Informationen zum Prozess an sich, sodass es hier nicht viel zu tun gibt. Wenn Sie WEITER anklicken, wird eine Seite angezeigt, auf der Sie gefragt werden, ob Sie einen neuen Transfer starten oder einen bereits gestarteten fortsetzen wollen (Abbildung 11.30). Wenn Sie Ihren alten Rechner bereits für die Dateiübertragung eingerichtet haben, dann wählen Sie die zweite Option, ansonsten die erste.

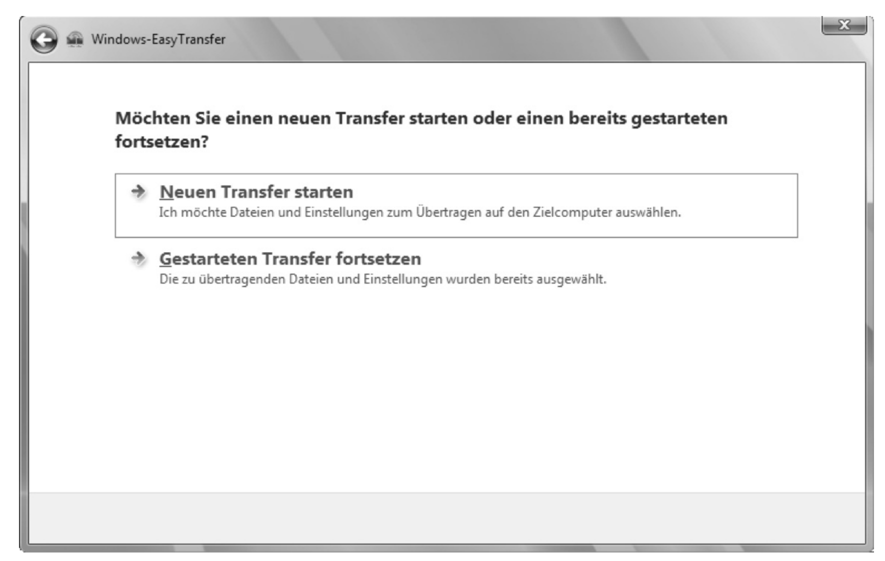


Abb. 11.30: Neuen Transfer starten oder Transfer fortsetzen?

Wenn Sie einen neuen Transfer starten, können Sie angeben, ob Sie Ihren neuen oder Ihren alten Computer verwenden. Folgen Sie dann den Anweisungen.

Umzugspraktiken

Wenn es bei Umzügen und Ausmusterungen um die Sicherheit geht, müssen Sie eine wichtige Frage beantworten: Was machen Sie mit dem alten System oder der Festplatte?

Man findet auf fast allen Laufwerken sensible Daten, außer vielleicht, wenn sie brandneu sind, und seien es einfache E-Mail-Nachrichten oder persönliche Aufzeichnungen, die bei einer Aufdeckung Peinlichkeiten verursachen könnten. Insbesondere im Arbeitsumfeld speichern die meisten Computer viele sensible Daten. Sie können nicht einfach nur `C:` formatieren und das Laufwerk dann weggeben.

Befolgen Sie beim Umzug oder bei der Ausmusterung eines Computers drei Grundsätze. Erstens, ziehen Sie mit den Benutzern und Daten in eine sichere Umgebung um. Solange Sie nicht alle Kennwörter korrekt zugewiesen und die Sicherheit des neuen Systems getestet haben, können Sie es nicht als sicher betrachten. Zweitens sollten Sie alle Datenreste von den Festplatten entfernen, die Sie lagern oder an gemeinnützige Organisationen verschenken wollen. Drittens sollten Sie alte Geräte korrekt entsorgen und keinesfalls in den Hausmüll werfen! PC-Recycler demontieren die Hardware und zerlegen Systemeinheiten, Tastaturen, Drucker und sogar Bildschirme so in ihre Bestandteile Kunststoff, Metall und Glas, dass diese wiederverwertet werden können.

Besonders leicht kann jemand sensible Daten kompromittieren oder darauf zugreifen, wenn er sich einfach an einen unbeaufsichtigten Rechner heranschleicht. Und wirklich einfach wird es, während gerade Daten auf ein neues, noch ungeschütztes System kopiert werden. Lassen Sie den Kopiervorgang nicht laufen, wenn Sie gerade zum Mittagessen gehen, sondern überwachen Sie ihn ununterbrochen und entfernen Sie alle Restdaten, die sich möglicherweise noch auf Massenspeichergeräten und insbesondere Festplatten befinden.

Datenvernichtung

Sie denken vermutlich, dass es ganz einfach sei, Daten loszuwerden – man verliert sie bisweilen ja auch ganz einfach versehentlich. Bei magnetischen Datenträgern wie Festplatten ist das jedoch nicht der Fall. Wenn Sie in Windows etwas löschen oder sogar den Papierkorb entleeren, bleiben die »gelöschten« Daten auf der Festplatte gespeichert (die Speicherbereiche werden in Windows als freier Platz angezeigt). Bei der Weitergabe oder Entsorgung einer Festplatte kann dies eine große Sicherheitslücke darstellen.

Tatsächlich ist es ziemlich schwierig, eine Festplatte wirklich vollständig zu löschen. Sie können Sie entweder physisch zerstören oder mit spezieller Software sicher löschen. Die Zerstörung ist nicht sonderlich kompliziert. Dazu gibt es Werkzeuge wie Schredder, Bohrmaschinen, Elektromagnete oder Entmagnetisierungsgeräte. Das Verbrennen oder Einschmelzen einer Festplatte ist eine zuverlässige Methode, die Daten zu löschen, aber gefährlich und nicht besonders umweltfreundlich. Denken Sie auch daran, dass Sie die Festplatte angesichts der hohen Speicherdichte in ziemlich kleine Stückchen zerlegen müssen, wenn Sie eine Wiederherstellung Ihrer Daten verhindern wollen.

Wichtig

Es gibt professionelle Dienstleister, die das Vernichten von Laufwerken mit einem Zertifikat garantieren. Man kann dann ruhig schlafen und muss sich keine Sorgen machen, dass wertvolle Daten in die falschen Hände geraten.

»Sicheres Löschen« einer Festplatte bedeutet, dass die Platte weiterhin funktioniert, sobald die Daten vernichtet sind. Es gibt hierfür einige mehr oder weniger wirksame Möglichkeiten. Für die CompTIA A+Prüfung müssen Sie den Unterschied zwischen einer normalen Formatierung und einer Lowlevel-Formatierung kennen. Die normale Formatierung kennen Sie bereits aus Kapitel 9, was also ist bei einer Lowlevel-Formatierung anders? Bei sehr alten (vor 1990 hergestellten) Festplatten wurden bei der Lowlevel-Formatierung die physikalischen Markierungen für die Datenaufzeichnung auf die Festplattenoberfläche geschrieben. Bei diesem Vorgang gehen die Daten verloren. Ursprünglich geschah das ausschließlich im Werk des Herstellers. Allerdings gab es auch bald Werkzeuge, mit denen sich

dieser Vorgang wiederholen ließ. Als die Laufwerke zunehmend komplexer wurden, haben die Hersteller die Möglichkeit einer Lowlevel-Formatierung außerhalb des Werks entfernt.

Heutzutage versteht man unter einer Lowlevel-Formatierung meistens das mehrfache Überschreiben mit Leerdaten. Dadurch soll die Festplatte in einen Zustand gebracht werden, der dem einer neuen Festplatte möglichst nahe kommt.

Sie können auch spezielle Löschprogramme verwenden, um alte, noch nicht überschriebene Daten endgültig zu löschen. Vereinfacht ausgedrückt werden mehrfach zufällige Daten auf die Platte geschrieben, weil die ursprünglichen Daten dann schwieriger wiederherzustellen sind. CCleaner von Piriform ist beispielsweise ein solches Programm, das den Webverlauf und Ihre letzten Aktivitäten unter Windows (etwa die zuletzt ausgeführten Programme) permanent löschen und Ihre Festplatte sogar derart »schrubben« kann, dass gelöschte Dateien nicht wiederhergestellt werden können (Abbildung 11.31).

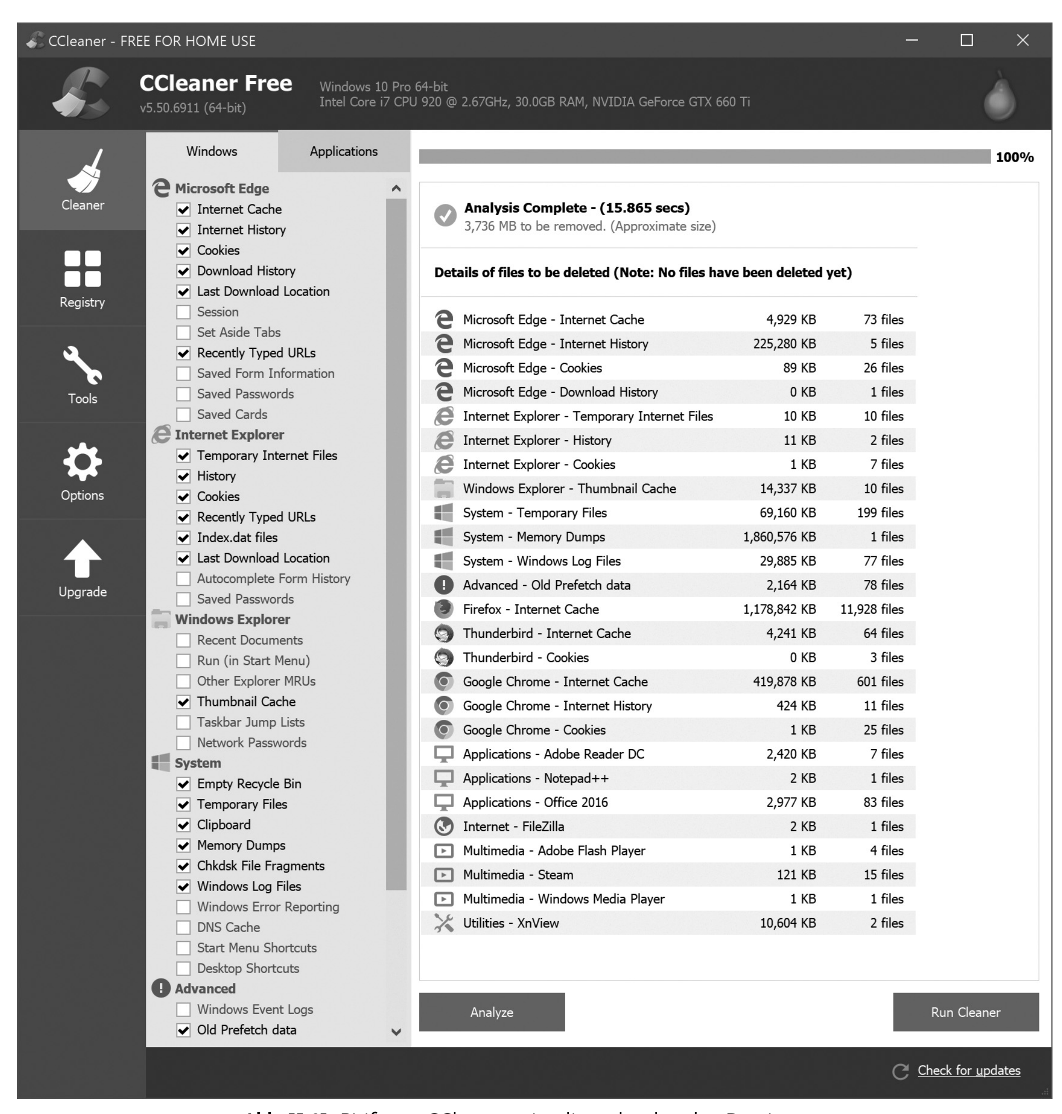


Abb. 11.31: Piriforms CCleaner zeigt die zu löschenden Dateien an.

Recycling

Recycling ist wichtig und hier können Sie als Computerbenutzer relativ leicht Ihr Umweltbewusstsein zeigen. Das Recycling von Produkten wie Papier, Tonerkartuschen oder Tintenpatronen sorgt nicht nur für weniger überfüllte Mülldeponien, sondern auch dafür, dass die giftigeren Inhaltsstoffe sicher und korrekt entsorgt werden. Die sichere Entsorgung von Hardware, die gefährliche Materialien enthält, wie etwa Bildschirme, schützt uns Menschen und die Umwelt.

Wer je versucht hat, einen Computer zu verkaufen, der älter als drei oder vier Jahre ist, hat die Lektion gelernt – sie sind nichts oder nicht mehr viel wert. Man ist dann wirklich versucht, diesen alten Computer einfach in den Müll zu werfen, aber das sollten Sie keinesfalls tun!

Erstens enthalten viele Computerkomponenten (z.B. Bildschirme) gefährliche Materialien, die die Umwelt verschmutzen. Glücklicherweise haben sich mittlerweile unzählige Unternehmen auf das Computer-Recycling spezialisiert und nehmen Ihnen Ihre alten Rechner gerne ab. Wenn Sie genügend alte Computer haben, werden Sie vielleicht sogar abgeholt. Wenn Sie kein Recycling-Unternehmen kennen, fragen Sie bei der städtischen Abfallentsorgung nach, wo man Ihnen mitteilen kann, wie Sie Ihr System am besten loswerden.

Noch besser ist es, wenn Sie Ihren alten Computer spenden. Viele Unternehmen suchen ständig nach Computern, die sie instand setzen und an Schulen oder andere Organisationen weitergeben können. Beachten Sie jedoch, dass der Computer in diesem Fall nicht zu alt sein sollte, denn nicht einmal Schulen wollen Computer, die älter als fünf oder sechs Jahre sind.

11.3.6 Keine Installation ist vollkommen

Auch wenn die Installation scheinbar reibungslos gelaufen ist, können doch allmählich Probleme auftauchen, insbesondere im Fall von Aktualisierungen. Sie müssen damit rechnen, dass die ein oder andere Anwendung neu installiert werden muss, oder dass Sie mit neuen Funktionen zu kämpfen haben, die es im vorherigen Betriebssystem nicht gab. Wenn alle Stricke reißen, können Sie zur alten Betriebssystemversion zurückkehren oder, falls Sie einen OEM-Computer (wie sie z.B. Dell und HP bauen) benutzen, gibt es auf der Festplatte des Rechners möglicherweise eine spezielle Partition zum Wiederherstellen, oder zumindest Installationsmedien (optische Discs oder USB-Speichersticks), die Sie dazu verwenden können, das Gerät wieder in den Auslieferungszustand zu versetzen. Eine Systemwiederherstellung wird normalerweise durch das Drücken einer bestimmten Taste – meistens F10 oder F11 – beim Booten eingeleitet. Folgen Sie danach den Anweisungen auf dem Bildschirm.

Die in diesem Kapitel beschriebenen Prozeduren sehen nach einer Menge Arbeit aus. Wie schlimm ist denn schon, sich eine Installations-Disc zu schnappen, eine Windows-Kopie auf ein System zu schubsen und die Dinge einfach laufen zu lassen? Reichlich schlimm! Das Verständnis dieser Vorgehensweisen ist nicht nur für die CompTIA A+-Zertifizierungsprüfung von Bedeutung. Sie können Ihnen sogar den, nun, Balg retten, wenn Sie als PC-Techniker tätig sind und die neueste Windows-Version auf dem neuen Rechner Ihres Chefs installieren müssen!

Jenseits von A+

11.4 Datenschutzbedenken bei Windows 10

All den positiven Aspekten von Windows 10 steht Microsofts beispielloser und fragwürdiger Umgang mit den persönlichen Daten der Benutzer gegenüber. Warum es scheinbar erforderlich ist, sich mit einem Microsoft-Benutzerkonto (Hotmail oder Outlook) bei Windows 10 anzumelden, ist eine der umstrittensten Fragen. Aufmerksame Techniker haben entdeckt, dass die Anmeldung mit einem Microsoft-Benutzerkonto es Windows ermöglicht, eine verstörend große Menge persönlicher Informationen zu übermitteln, wie beispielsweise das Kennwort Ihres WLANs. Sicherheitsbewusste Benutzer sollten es in Betracht ziehen, ein lokales Benutzerkonto alter Schule einzurichten. Wenn Sie sich

nicht mit einem Microsoft-Benutzerkonto anmelden, funktioniert allerdings die Sprachassistentin Cortana nicht mehr.

Neben der Anmeldung mit einem Microsoft-Benutzerkonto gibt es eine Reihe weiterer den Datenschutz betreffende Probleme. Sie sollten es in Betracht ziehen, die nachfolgend aufgeführten Funktionalitäten zu deaktivieren. Die meisten davon können in der Einstellungs-App im Bereich DATENSCHUTZ abgeschaltet werden.

- **Apps die Verwendung der Werbungs-ID für App-übergreifende Erlebnisse erlauben**: Damit räumen Sie Microsoft das Recht ein, eine einzigartige Werbungs-ID zu erstellen, zu nutzen und weiterzugeben, die mindestens zu personalisierter Werbung auf Webseiten führt.
- **Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktion in Zukunft zu verbessern**: Den genauen Zweck dieser Option erläutert Microsoft nirgends, aber es reicht wohl aus festzustellen, dass alle Tastatureingaben mitgeschnitten werden können. Gruselig!
- **Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen**: Warum muss Microsoft auf die Spracheinstellungen zugreifen, wenn doch jede Website problemlos die Standardsprache ermitteln kann? Wenn Sie nicht mehr als eine Sprache verwenden, sollten Sie diese Funktion deaktivieren.
- **Position**: Die Ortungsdienste ermöglichen es Microsoft, Ihren Aufenthaltsort zu ermitteln, wenn Sie diese Einstellung nicht deaktivieren.
- **Mich kennenlernen**: Diese freundlich klingende Funktion sammelt jede Menge Daten über Sie, wie z.B. Kontakte, Kalendereinträge, Sprache, Handschrift usw. Schalten Sie diese Funktion besser aus.

Man kann es so zusammenfassen: Windows 10 ist einfach zu benutzen und bietet eine Vielzahl an Funktionen. Sie haben die Möglichkeit, den Datenschutz auf Wunsch zu verbessern.

11.5 Wiederholung

11.5.1 Fragen

1. Was ist ein Thin-Client?
   A. Ein Computer mit 32 Bit breitem Adressbus
   B. Ein tragbarer Computer
   C. Ein Computer, der dafür ausgelegt ist, nur die grundlegendsten Anwendungen auszuführen, und dessen Hardware gerade die minimalen Systemanforderungen des Betriebssystems erfüllt
   D. Ein Computer mit sehr schlankem Gehäuse
2. Welche Aufgaben erfüllt ein NAS-Gerät? (Wählen Sie drei Antworten aus.)
   A. Medienstreaming
   B. Dateifreigabe
   C. Webdienste
   D. Druckerfreigabe
3. Sonjas Kunde möchte einen Arbeitsplatzrechner zur Bildverarbeitung beschaffen. In seinem Netzwerk sind zehn Arbeitsplatzrechner zu einer Windows-Domäne zusammengeschlossen, und der neue Rechner soll Teil dieser Domäne werden. Welche Edition von Windows 10 sollte Sonja auf dem Computer installieren, um dieses Ziel möglichst preisgünstig zu erreichen?
   A. Windows 10 Starter Edition
   B. Windows 10 Home
   C. Windows 10 Pro
   D. Windows 10 Enterprise

4. Was ist bei einem Arbeitsplatzrechner mit virtuellen Maschinen entscheidend?
   A. CPU
   B. Netzteil
   C. RAM
   D. Großer Bildschirm
5. Welches Werkzeug ermöglicht es, Windows über ein Netzwerk zu installieren?
   A. Windows-DVD
   B. NetBoot
   C. PXE
   D. Windows kann nicht über ein Netzwerk installiert werden.
6. Wie installieren Sie neben einem bereits vorhandenen Betriebssystem ein weiteres?
   A. Durch Neuinstallation
   B. Durch Upgrade-Installation
   C. Durch Multiboot-Installation
   D. Durch Netzwerkinstallation
7. Was passiert mit Ihrem Computer, wenn Sie die Windows-Aktivierung nicht durchführen?
   A. Nichts. Die Aktivierung ist optional.
   B. Der Computer funktioniert 30 Tage lang problemlos, anschließend wird Windows deaktiviert.
   C. Microsoft weiß nicht, wie es Sie erreichen soll, um Ihnen Upgrade-Informationen bereitzustellen.
   D. Er funktioniert weiter, wenn man das Kontrollkästchen ICH BEZAHLE WINDOWS SPÄTER aktiviert.
8. Was sollten Sie tun, wenn Windows während der Installation abstürzt?
   A. Sie drücken `Strg` + `Alt` + `Entf`, um den Installationsprozess neu zu starten.
   B. Sie drücken den Reset-Schalter, um den Installationsprozess neu zu starten.
   C. Sie drücken `ESC`, um den Installationsprozess abzubrechen.
   D. Sie ziehen den Netzstecker und starten den Installationsprozess neu.
9. Welcher Begriff beschreibt eine Zusammenstellung vieler Aktualisierungen und Korrekturen für Windows?
   A. Hotfix
   B. Hotpack
   C. Service Pack
   D. Service Release
10. Sie haben gerade Ninas PC mit Windows 7 durch einen neuen PC mit Windows 10 ersetzt. Welche Werkzeuge sollten Sie nach der Installation ausführen, damit der Umzug auf das System für sie möglichst reibungslos abläuft?
   A. Windows-Aktivierung
   B. Reparaturinstallation
   C. Windows-EasyTransfer
   D. User State Migration Tool

11.5.2 Antworten

1. **C.** Ein Thin-Client ist ein Computer, der nur die grundlegendsten Anwendungen ausführt und auf einen Server angewiesen ist, um größere Aufgaben zu erledigen.
2. **A, B, D.** Ein NAS-Gerät dient zum Medienstreaming sowie zur Datei- und Druckerfreigabe.
3. **C.** Windows 10 Pro ist hier die beste Wahl. Die Enterprise-Edition würde auch funktionieren, ist aber teurer und besitzt Features, die der Kunde nicht braucht.
4. **C.** Jede virtuelle Maschine benötigt eine Menge Arbeitsspeicher, daher können Sie mehr virtuelle Maschinen betreiben, wenn mehr RAM vorhanden ist.
5. **C.** PXE (*Preboot Execution Environment*) ermöglicht es, Windows über ein Netzwerk zu installieren.
6. **C.** Durch die Installation eines weiteren Systems entsteht ein Multiboot-System.
7. **B.** Wenn Sie die Aktivierung von Windows nicht durchführen, funktioniert der Computer 30 Tage lang problemlos, anschließend wird Windows deaktiviert.
8. **D.** Wenn Windows während der Installation abstürzt, sollten Sie den Netzstecker ziehen und den Installationsvorgang neu starten.
9. **C.** Ein Service Pack ist eine Zusammenstellung vieler Updates und Patches für Windows.
10. **C.** Führen Sie Windows-EasyTransfer aus, um all ihre persönlichen Dateien und vertrauten Einstellungen (Desktopgestaltung usw.) auf den neuen Rechner mit Windows 10 zu übertragen.

Windows unter der Haube 12

Themen in diesem Kapitel:

- Die Registry
- Der Windows-Startvorgang im Detail
- Prozesse, Dienste und Threads
- Dienst- und Hilfsprogramme für Programmierer

Windows ist leistungsfähig, einfach zu benutzen, erstaunlich idiotensicher, abwärtskompatibel und stabil. Ein großer Teil von Windows bleibt dem normalen Benutzer jedoch verborgen. Es gibt viele Programme und Prozesse, die sozusagen »unter der Haube« ausgeführt werden. Ich möchte hier klarstellen, dass ich es für eine pfiffige Idee halte, die Teile des Systems, auf die einfache Benutzer nicht zugreifen müssen, zu verstecken. Techniker hingegen müssen diese Programme und Prozesse nicht nur verstehen, sondern auch verwenden, konfigurieren und bei Bedarf reparieren können. Wir sehen uns in diesem Kapitel die Registry (auch Registrierung oder Registrierungsdatenbank genannt), den Windows-Startvorgang, Prozesse, Dienste und Threads sowie für Programmierer nützliche Werkzeuge an.

1002

12.1 Die Registry

Die *Registry* ist eine riesige Datenbank, in der Informationen über den Rechner gespeichert werden, wie z.B. über Hardwarekomponenten, das Netzwerk, Benutzereinstellungen, Dateitypen, Kennwörter, Desktop-Hintergrundfarbe und praktisch alle anderen Windows-Elemente. Bei fast allen Konfigurationsvorgängen an einem Windows-System wird die Registry geändert. Sie ist von entscheidender Bedeutung – ohne sie kann Ihr System Windows nicht starten.

Unter allen Windows-Versionen befinden sich die verschiedenen Registry-Dateien (oder Registrierungsstrukturen, die sogenannten *hives*) im Ordner `%SystemRoot%\System32\config` und in allen Benutzerordnern. Glücklicherweise müssen Sie auf diese ziemlich großen Dateien nur selten direkt zugreifen. Stattdessen können Sie eine Reihe relativ benutzerfreundlicher Anwendungen zur Bearbeitung der Registry benutzen.

Erstaunlicherweise kommt die Registry in den Lernzielen der CompTIA A+-Zertifizierung nicht vor. Sie sollten aber die Basiskomponenten der Registry verstehen und müssen wissen, wie Sie Daten in der Datenbank manuell ändern und bestimmte Einstellungen finden können. Und die CompTIA sollte das in den Lernzielen aufnehmen!

12.1.1 Zugriff auf die Registry

Obwohl die Registry von so großer Bedeutung ist, greift man nur selten direkt darauf zu. Aber wenn Sie die Windows-Einstellungs-App oder die Systemsteuerung (oder so ziemlich jedes andere Hilfsprogramm) verwenden, bearbeiten Sie tatsächlich die Registry. Es gibt jedoch Situationen, in denen Techniker direkt darauf zugreifen müssen.

Bevor Sie einen Blick in die Registry werfen können, sehen wir uns erst einmal an, wie Sie mit dem Registrierungs-Editor direkt darauf zugreifen können, damit Sie die Datenbank auf Ihrem Rechner öffnen und mit den Beispielen in diesem Kapitel vergleichen können. Geben Sie in das Suchfeld im Startmenü `regedit` ein, um den Registrierungs-Editor zu öffnen. Sie können diesen Befehl auch auf der Kommandozeile eingeben.

12.1.2 Der Aufbau der Registry

Die Registry ist ähnlich wie die Ordner auf der Festplatte in Form einer Baumstruktur aufgebaut. Nach dem Start des Registrierungs-Editors sehen Sie fünf Hauptgruppen bzw. *Hauptschlüssel*:

- `HKEY_CLASSES_ROOT`
- `HKEY_CURRENT_USER`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG`

Versuchen Sie einmal, einen dieser Hauptschlüssel zu öffnen, indem Sie das Aufklappsymbol links neben dem Eintrag anklicken, und beachten Sie dabei, dass sich darunter weitere Unterschlüssel befinden. Ein Unterschlüssel kann weitere Unterschlüssel bzw. *Werte* besitzen. Abbildung 12.1 zeigt ein Beispiel eines Unterschlüssels mit Werten. Beachten Sie, dass der Registrierungs-Editor Schlüssel auf der linken und die Werte auf der rechten Seite anzeigt. Alle diese Hauptschlüssel erfüllen eine spezielle Funktion, deshalb werden wir sie nachfolgend einzeln betrachten.

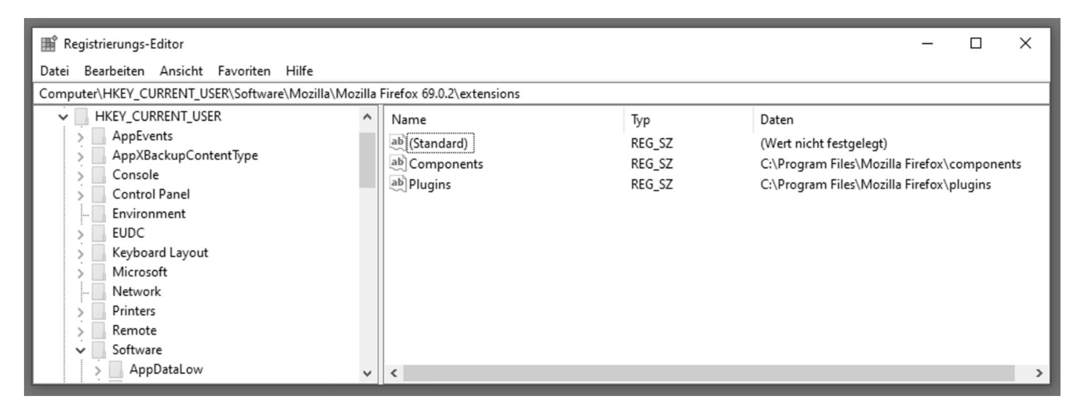


Abb. 12.1: Typische Schlüssel und Werte in der Registry

HKEY_CLASSES_ROOT

Dieser Hauptschlüssel definiert die von Windows verwendeten Standard-Klassenobjekte. Ein *Klassenobjekt* ist eine benannte Funktionsgruppe, die definiert, was Sie mit dem von ihr dargestellten Objekt machen können. Beispielsweise sind fast alle der Funktionen, die mit Dateien auf dem System zu tun haben, über ein solches Klassenobjekt festgelegt. So definiert die Registry z.B. JPG-Bilddateien unter Verwendung von zwei Klassenobjekten. Ein Objekt befindet sich unter `HKEY_CLASSES_ROOT\.jpg` und eines unter `HKEY_CURRENT_USER\Software/Classes\.jpg`, das benutzerdefinierte Zuordnungen von JPG-Dateien enthält. Heute kombiniert dieser Hauptschlüssel Klassenobjekte des Typs `\Software\Classes`, die zu den Hauptschlüsseln `HKEY_CURRENT_USER` und `HKEY_LOCAL_MACHINE` gehören, um abwärtskompatibel mit älteren Anwendungen zu sein.

HKEY_CURRENT_USER und HKEY_USERS

Windows kann so konfiguriert werden, dass es mehrere Benutzer eines Rechners unterstützt und alle benutzerspezifischen Einstellungen wie Bildschirmfarben, Bildschirmschoner und Inhalt des Desktops für jeden Benutzer mit Benutzerkonto auf dem System getrennt speichert. `HKEY_CURRENT_USER` speichert die aktuellen Benutzereinstellungen und `HKEY_USERS` alle personalisierten Informationen der Benutzer eines Rechners. Sie können hier zwar Dinge wie den Bildschirmschoner ändern, aber es ist in jedem Fall besser, den Desktop mit der rechten Maustaste anzuklicken und ANPASSEN zu wählen!

HKEY_LOCAL_MACHINE

Dieser Hauptschlüssel enthält alle Daten eines Systems, die nicht benutzerspezifisch sind. Hierzu gehören unter anderem alle Geräte und Programme eines Rechners.

HKEY_CURRENT_CONFIG

Falls Werte in `HKEY_LOCAL_MACHINE` über mehr als nur eine Option verfügen (wie es beispielsweise bei zwei Bildschirmen der Fall ist), definiert dieser Hauptschlüssel, welche der Optionen aktuell verwendet wird. Da die meisten Leute nur über einen Monitor oder eine ähnliche Ausstattung verfügen, ist dieser Bereich meist uninteressant.

Tipp

Sehen Sie sich unbedingt die drei tollen Übungen zum Thema »Speicherorte der Registry« unter `http://totalsem.com/100x` an. Die Kombination aus Tippen, Anzeigen und Klicken bereitet Sie auf alle Fallbeispiele vor, in denen es um die Registry geht.

12.1.3 Verwendung der Registry

Bei der Beschreibung der Registrierungs-Einstellungen wird eine bestimmte Notation benutzt. Ich habe beispielsweise kürzlich meine Kopie von *World of Warcraft* von Laufwerk `C:` auf Laufwerk `D:` verschoben und hatte danach Schwierigkeiten beim Start des Programms. Auf den Webseiten von Blizzard Entertainment (`http://www.blizzard.com`), dem Hersteller des Programms, habe ich dann den Support kontaktiert, der mir folgende Anweisung gab: »Gehen Sie in der Registry zu `HKLM\SOFTWARE\Blizzard Technologies\World of Warcraft` und ändern Sie die Objekte `GamePath` und `InstallPath`, sodass sie auf den neuen Speicherort des Spiels verweisen.«

Ich habe also den Registrierungs-Editor gestartet und konnte dank dieser Notation die Registrierungs-Einstellungen auffinden (Abbildung 12.2). Vergleichen Sie die Abbildung mit der Anleitung von Blizzard. Beachten Sie, dass `HKEY_LOCAL_MACHINE` als `HKLM` abgekürzt ist.

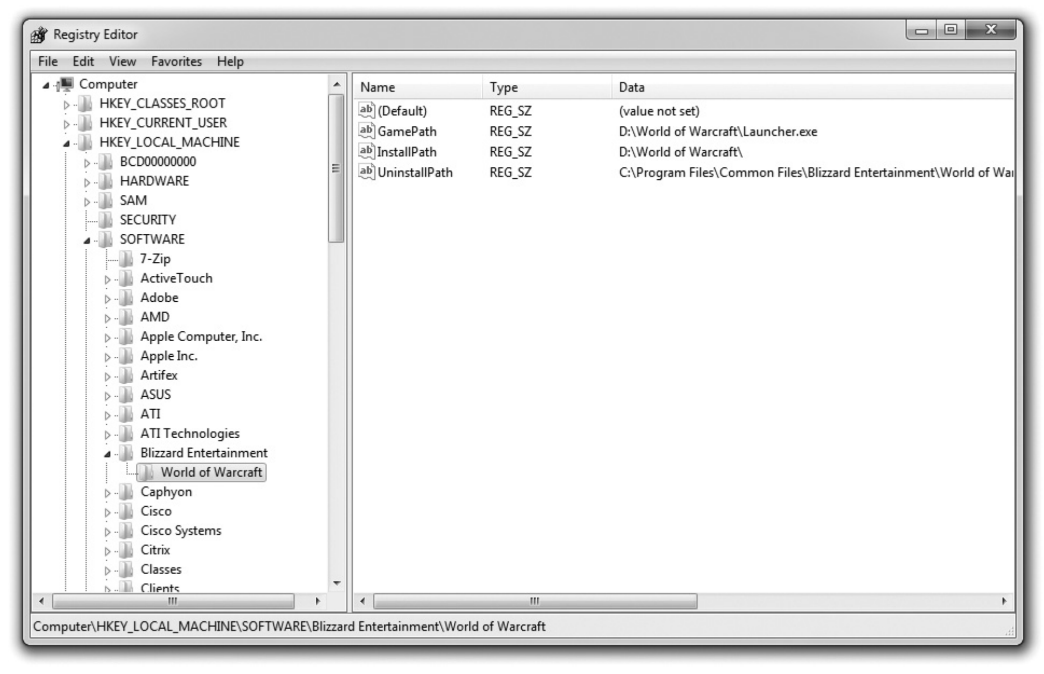


Abb. 12.2: Bearbeiten der Registry

Im Beispiel ist `World of Warcraft` ein Unterschlüssel von `Blizzard Entertainment`. Dieses Objekt ist seinerseits ein Unterschlüssel von `SOFTWARE` und dieser wiederum ein Unterschlüssel des Hauptschlüssels `HKLM`. Der Schlüssel `World of Warcraft` besitzt vier Unterschlüssel. Alle Schlüssel besitzen normalerweise einen Standardwert (*Default*). Im Beispiel sind drei der Werte geändert worden.

Jeder Wert muss von einem bestimmten Typ sein:

- **Zeichenkette**: Dieser Typ ist am flexibelsten und sehr gebräuchlich. Hier können Sie alle möglichen Arten von Daten speichern.
- **Binärzahlen**: Hier werden ausschließlich aneinandergereihte Einsen und Nullen gespeichert.
- **DWORD-Werte**: Ähnlich den Binärzahlen, jedoch auf exakt 32 Bit beschränkt.
- **QWORD-Werte**: Ebenfalls den Binärzahlen ähnlich, allerdings auf genau 64 Bit beschränkt.

Es gibt noch weitere Datentypen, aber diese vier werden in den allermeisten Registry-Einstellungen verwendet.

12.1.4 Manuelle Änderung der Registry

Es gibt nur selten einen Grund, die Registrierungs-Einstellungen von Hand zu ändern, wenn Sie nicht gerade Nachforschungen angestellt haben und Ihnen dazu geraten wird. Beim Ändern der Registry laufen Sie Gefahr, bestimmte Windows-Funktionen unbrauchbar zu machen: Programme starten nicht, Dienstprogramme funktionieren nicht, oder schlimmstenfalls startet der Rechner nicht mehr. Um derartige Probleme zu verhindern, sollten Sie immer eine Sicherheitskopie der Registry erstellen, bevor Sie irgendetwas ändern. Sobald sich die Sicherheitskopie an einem sicheren Ort befindet (ich verwende einen USB-Speicherstick), können Sie die Änderung vornehmen und den Rechner neu starten, um zu prüfen, ob durchgeführten Änderungen den gewünschten Effekt erzielen. Wenn alles funktioniert: wunderbar! Anderenfalls müssen Sie die alten Registrierungs-Einstellungen wiederherstellen. Genau das werden wir nun tun.

Das Löschen von Autostart-Programmen gehört zu den häufigeren Aktionen, die mit dem Registrierungs-Editor durchgeführt werden. Ich möchte verhindern, dass drei Programme, die zusammen mit meiner Logitech-GamePanel-Tastatur und -Maus installiert worden sind, automatisch gestartet werden. Der übliche Ort zum Vornehmen einer solchen Änderung ist

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Wenn Sie den Registrierungs-Editor starten und diesen Schlüssel anzeigen, sollte das etwa wie in Abbildung 12.3 aussehen.

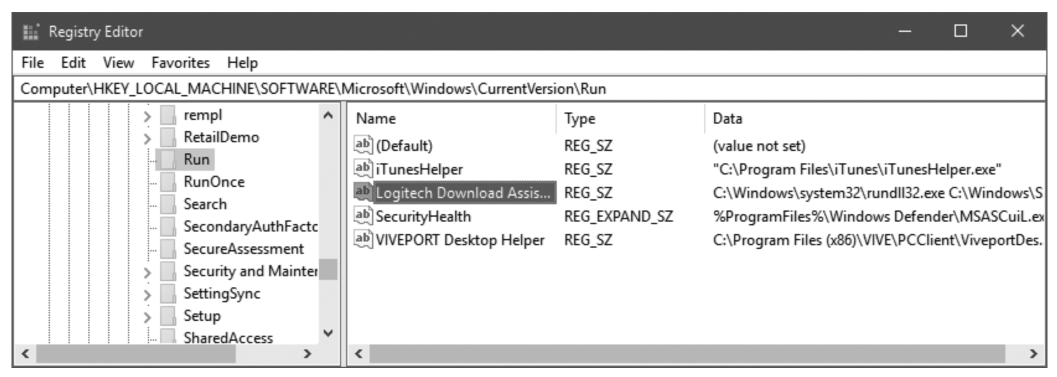


Abb. 12.3: Der Unterschlüssel RUN

Vor dem Löschen der Schlüssel werde ich eine Kopie meiner Registry speichern. Mit der Funktion des Registry -Editors zum Exportieren können Sie die gesamte Registry oder einen einzelnen Haupt- bzw.

Unterschlüssel (inklusive aller untergeordneten Schlüssel und Werte) speichern. Wählen Sie dazu den Unterschlüssel RUN aus und klicken Sie im Menü DATEI auf den Eintrag EXPORTIEREN. Speichern Sie den Unterschlüssel mit der Dateierweiterung `.reg` ab und merken Sie sich gut, wo Sie die Datei ablegen. Falls Sie den Schlüssel wiederherstellen müssen, verwenden Sie dazu den Befehl DATEI|IMPORTIEREN oder klicken Sie, wie in Abbildung 12.4, mit der rechten Maustaste auf die exportierte Datei und wählen Sie ZUSAMMENFÜHREN aus.



Abb. 12.4: Import der Run-Schlüssel aus einer Sicherheitskopie

12.1.5 Kommandozeilenprogramme zur Bearbeitung der Registry

Windows bringt einige Werkzeuge zum Bearbeiten der Registry auf der Kommandozeile mit (und viele weitere für die PowerShell). Die beiden, die Sie hin und wieder benötigen werden, heißen `reg` und `regsvr32`.

Hinweis

Wenn die Eingabeaufforderung Neuland für Sie ist, können Sie diesen Abschnitt zunächst überspringen und nach der Lektüre von Kapitel 15, *Eingabeaufforderung*, zu ihm zurückkehren.

Der Befehl `reg` ist ein vollwertiges Werkzeug zum Bearbeiten der Registry. Sie können damit Schlüssel und Werte anzeigen, ausgewählte oder alle Schlüssel importieren und exportieren und sogar zwei verschiedene Versionen der Registry miteinander vergleichen. Der Befehl ist derart leistungsfähig, dass er über mehrere Hilfe-Ebenen verfügt, sodass Sie sich Kommandos zusammenstellen können, mit denen die Registry ganz gezielt bearbeitet werden kann. Beispielsweise zeigt der Befehl `reg /?` eine Liste von 12 Aktionen an (wie z.B. `req query /?` oder `reg add /?`), für die Sie sich die Hilfe anzeigen lassen können.

Der Befehl `regsvr32` hingegen kann die Registry nur auf eine einzige Weise ändern. Er dient zum Hinzufügen (oder zum *Registrieren*) von DLL-Dateien (Dynamic Link Library). Wenn Sie das Programm `regsrv32` unter einer 64-Bit-Version von Windows starten, wird die 64-Bit-Version aufgerufen. Das kann zu Problemen führen, wenn Sie versuchen, der Registry eine 32-Bit-DLL hinzuzufügen. Um das zu tun, müssen Sie die Datei `regsvr32.exe` im Ordner `%SystemRoot%Syswow64` ausführen.

Falls Sie wider Erwarten jemals `reg` oder eine der beiden `regsvr32`-Versionen ausführen müssen, können Sie in Kapitel 15 nachlesen, wie sich die Eingabeaufforderung effizient nutzen lässt.

12.2 Der Startvorgang

Während der Installation werden eine Reihe Windows-spezifischer Dateien und Ordner erstellt, die das Betriebssystem benötigt, um auf einem Rechner laufen zu können. Einige dieser Dateien und Ordner befinden sich direkt im Stammverzeichnis auf Laufwerk `C:`, andere befinden sich an anderen Stellen im Dateisystem. Die Position dieser Dateien und Ordner können Sie sich am besten merken, wenn Sie wissen, wie wichtig sie für das Betriebssystem sind und welche Rolle sie beim Rechnerstart spielen.

Aktuelle Windows-Versionen können über BIOS oder via UEFI booten. Direkt nach dem Einschalten des Systems wird entweder das BIOS oder das UEFI gestartet. Der Unterschied zwischen BIOS- und UEFI-Systemen besteht darin, was anschließend geschieht.

- Bei einem BIOS-basierten System sucht das BIOS in der festgelegten Startreihenfolge auf den Partitionen nach einem *MBR*. Der MBR enthält einen kleinen Teil des Dateisystem-Bootcodes, der die Partitionstabelle des Systems nach der Systempartition durchsucht und dann deren Bootsektor lädt. Der Bootsektor wiederum enthält Code, der eigentlich nur den Bootprozess an eine Datei namens `bootmgr` (den Bootmanager) übergibt. Kurz und bündig: Das BIOS sucht nach dem MBR, der den Code zum Start des Betriebssystems findet.
- Auf einem UEFI-System wird hingegen weder der Code des MBR/GUID-Partitionsschemas (GPT) noch der Dateisystem-Bootcode ausgeführt. Das UEFI lädt `bootmgr` einfach direkt.

Hinweis

`bootmgr` befindet sich auf der speziellen, für das System reservierten Partition, die Sie in Kapitel 9 kennengelernt haben. Wenn Sie ein UEFI-System verwenden, so gibt es dort eine sinnvollerweise als EFI benannte Systempartition, auf der sich eine spezielle Version des `bootmgr` namens `bootmgr.efi` befindet.

Wenn der Bootmanager gestartet wird, liest er die *Boot-Konfigurationsdaten* (*BCD – Boot Configuration Data*), die neben Informationen über die verschiedenen auf dem System installierten Betriebssysteme Angaben darüber enthält, wie diese tatsächlich geladen werden können (Bootstrap). Wenn ein Betriebssystem ausgewählt wurde (oder sofort, wenn nur eines vorhanden ist), lädt `bootmgr` ein Programm namens `winload.exe`, das Ihr System auf das Laden des Betriebssystemkerns (`ntoskrnl.exe`) selbst vorbereitet. Das ähnelt ein wenig dem Hausputz vor dem Besuch von Tante Erna. Dabei lädt `bootmgr` die Hardware-Abstraktionsschicht, die Systemregistrierung und die Treiber für die Bootgeräte in den Arbeitsspeicher, bevor das Betriebssystem selbst die Kontrolle übernimmt.

Hinweis

Wenn Sie Windows schon länger benutzen, ist Ihnen vielleicht schon einmal eine Fehlermeldung begegnet, die besagt, dass Windows nicht gestartet werden kann, weil `bootmgr` fehlt. Diese Meldung erscheint, wenn der Bootsektorcode `bootmgr` nicht finden kann. Gründe hierfür können ein defektes Dateisystem, eine durcheinandergewürfelte Installation oder Viren sein.

Sobald der *Betriebssystemprozess* (`ntoskrnl.exe`) übernimmt, lädt er alle verschiedenen Prozesse und Komponenten des Windows-Betriebssystems. Dann wird das Windows-Logo angezeigt und Sie können sich glücklich schätzen und mit der Arbeit am Rechner beginnen, ohne von den ganzen komplizierten elektronischen Vorgängen Notiz zu nehmen, die gerade im Rechner stattgefunden haben.

12.3 Anwendungen, Prozesse und Dienste

In Kapitel 3, *Mikroprozessoren*, haben Sie erfahren, dass CPUs Threads ausführen, einzelne Programmteile, die der CPU bereitgestellt werden. Nun wollen wir uns die Sache aus der Sicht von Windows ansehen.

Hinweis

Ich werde die Zusammenhänge für die CompTIA A+Prüfung etwas vereinfachen. Sie sollen aber wissen, dass Anwendungen, Prozesse und Dienste erheblich komplizierter sein können als hier dargestellt.

Programme sind in Windows ausführbare Dateien, die sich auf einem Massenspeichergerät befinden. Wenn Sie ein Programm starten, lädt Windows es in Form eines Prozesses in den Arbeitsspeicher. Die CPU erkennt den Prozess und dieser teilt der CPU mit, welche Codeteile ausgeführt werden sollen. Der Umgang mit Prozessen in ihren verschiedenen Formen hat wesentlichen Anteil am Verständnis dessen, was unter der Haube vor sich geht.

Bei Windows handelt es sich um ein Multitasking-Betriebssystem, das viele verschiedene Prozesse gleichzeitig ausführt. Viele dieser Prozesse laufen in Fenstern (oder bildschirmfüllend) ab, wenn Sie diese starten, und werden beendet, wenn Sie das Fenster wieder schließen. Solche Prozesse werden als *Anwendungen* bezeichnet. Es gibt jedoch noch eine andere Art von Prozessen, die für die Erledigung ihrer Aufgaben keine Fenster benötigen. Diese Prozesse laufen unsichtbar im Hintergrund und stellen viele nützliche Funktionen bereit. Sie werden in ihrer Gesamtheit *Dienste* genannt. Lassen Sie uns nun Anwendungen, Dienste und die Werkzeuge um sie zu steuern genauer betrachten.

12.3.1 Task-Manager

Der *Task-Manager* ist die erste Anlaufstelle für alle möglichen Dinge, die Sie mit Anwendungen, Prozessen und Diensten anstellen können (Abbildung 12.5). Die Entwickler bei Microsoft haben den Task-Manager für Windows 8 maßgeblich überarbeitet. Wir sehen uns das Werkzeug zunächst unter Windows 7 an und betrachten dann den Task-Manager unter Windows 8/8.1/10.

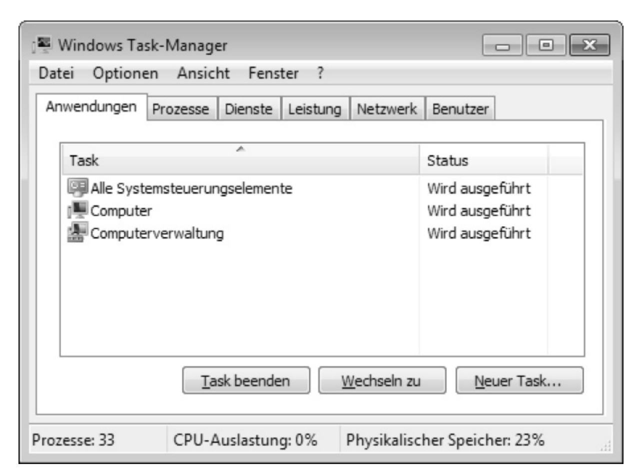


Abb. 12.5: Der Task-Manager in Windows 7

Der Task-Manager in Windows 7

Am schnellsten lässt sich der Task-Manager über `Strg` + `⇧` + `ESC` aufrufen. Es gibt zwei weitere Methoden, die Ihnen in den CompTIA A+-Prüfungen begegnen können: Wählen Sie START|AUSFÜHREN oder START|SUCHEN, geben Sie `taskmgr` ein und drücken Sie `↵` oder drücken Sie `Strg` + `Alt` + `Entf` und wählen Sie TASK-MANAGER aus.

Anwendungen Auf der Registerkarte ANWENDUNGEN werden alle auf Ihrem System laufenden Anwendungen angezeigt. Falls sich eine davon nicht auf die übliche Art beenden lässt, ist dies der richtige Ort, um ein Programm sofort zu beenden. Wählen Sie es aus und klicken Sie auf TASK BEEN-

DEN. Sie können dazu auch die rechte Maustaste und das Kontextmenü verwenden. Seien Sie aber vorsichtig mit dieser Funktion! Eine Abfrage wie »Sind Sie sicher?« gibt es hier nicht und schnell hat man versehentlich die falsche Anwendung beendet.

Auf der Registerkarte Anwendungen gibt es zwei weitere praktische Schaltflächen:

- Mit WECHSELN ZU können Sie ein beliebiges Programm in den Vordergrund bringen. Äußerst praktisch, wenn Sie sehr viele Anwendungen geöffnet haben.
- NEUER TASK ist ein klasse Werkzeug, um ein beliebiges Programm zu starten, sofern Sie dessen Dateinamen kennen. Klicken Sie auf NEUER TASK, geben Sie `cmd` ein und drücken ↵, um beispielsweise die Eingabeaufforderung zu öffnen.

Beachten Sie hier, dass alles ein Prozess ist. Alle Anwendungen sind daher auch auf der Registerkarte PROZESSE aufgeführt. Klicken Sie mit der rechten Maustaste auf eine Anwendung und wählen Sie dann ZU PROZESS WECHSELN aus, um zur Registerkarte PROZESSE zu gelangen und sich anzeigen zu lassen, welcher Prozess die Anwendung ausführt.

Prozesse Wenn Sie den Task-Manager wirklich ausreizen wollen, dann klicken Sie auf die Registerkarte PROZESSE (Abbildung 12.6). Da alles ein Prozess ist und auf der Registerkarte PROZESSE sämtliche Prozesse angezeigt werden, sehen Sie hier tatsächlich alles, was gerade auf Ihrem Computer ausgeführt wird.

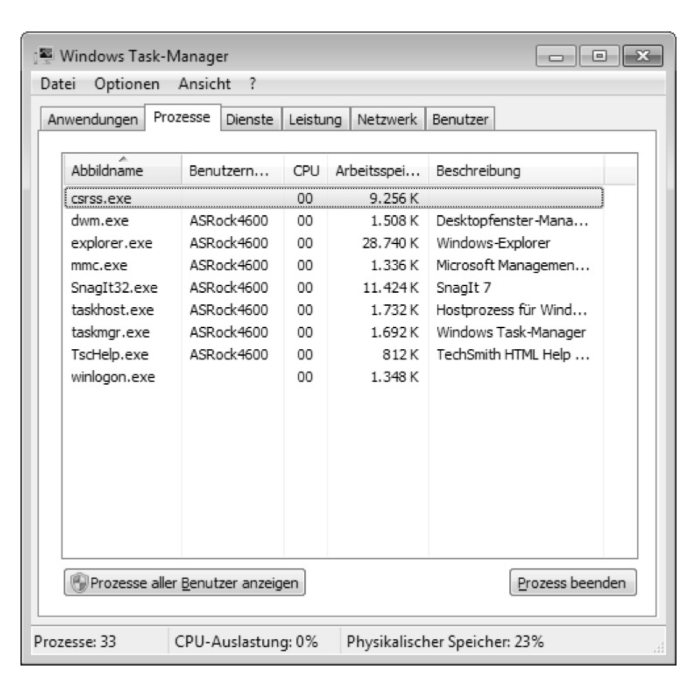


Abb. 12.6: Registerkarte PROZESSE in Windows 7

Alle Prozesse besitzen bestimmte gemeinsame Eigenschaften, die Ihnen wohlbekannt sein dürften:

- Ein Prozess wird nach seiner ausführbaren Datei benannt, deren Name meist auf `.exe` endet, dies aber nicht notwendigerweise muss.
- Jedem Prozess ist ein Benutzername zugeordnet, damit erkennbar ist, wer den Prozess gestartet hat. Von Windows gestarteten Prozessen wird der Name `SYSTEM` zugewiesen.
- Jeder Prozess besitzt eine *PID* (*Process Identifier*). Zur Identifizierung eines Prozesses wird dessen PID benutzt, nicht dessen Name. Standardmäßig zeigt der Task-Manager die PID nicht an. Kli-

cken Sie auf ANSICHT|SPALTEN AUSWÄHLEN und markieren Sie PID (PROZESS-ID), um diese anzuzeigen (Abbildung 12.7).

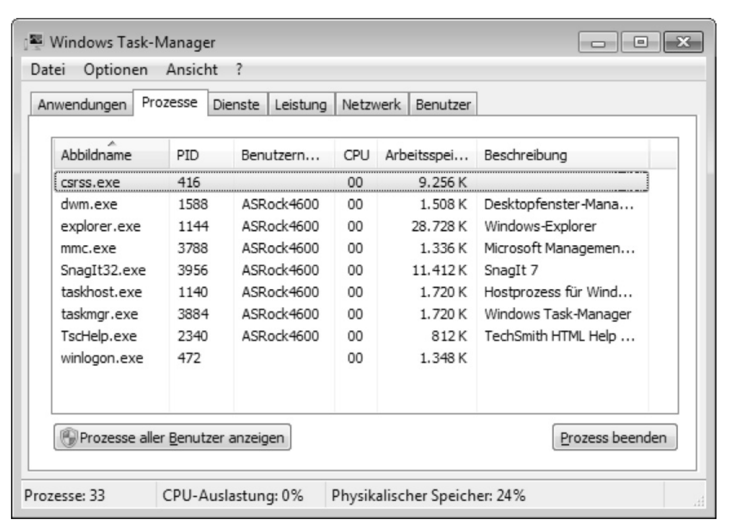


Abb. 12.7: Registerkarte PROZESSE mit PID-Spalte in Windows 7

Der Task-Manager zeigt wichtige Informationen über Prozesse an. Dazu gehören unter anderem die CPU-Auslastung in Prozent und die Menge des Arbeitsspeichers (in Kilobyte), die der Prozess belegt. Viele Prozesse liefern außerdem eine Beschreibung, was genau der Prozess eigentlich macht, allerdings müssen Sie vermutlich nach rechts scrollen, um diese Informationen anzuzeigen (Abbildung 12.8).

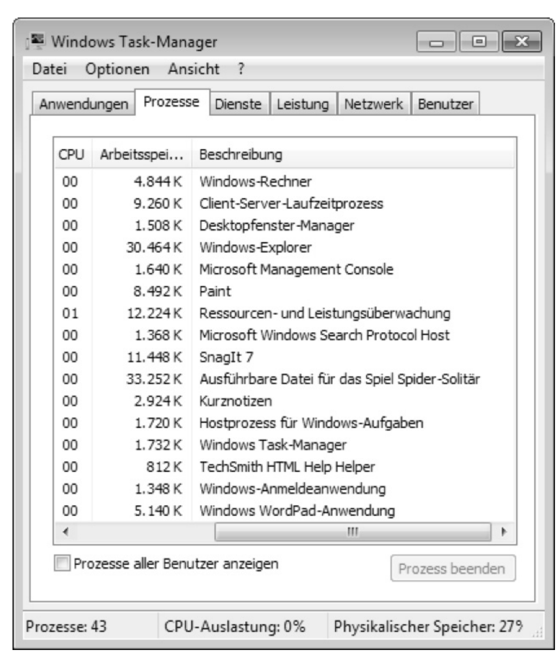


Abb. 12.8: Details zu den Prozessen in Windows 7

Sie werden bemerkt haben, dass fast alle Prozesse nur einem Benutzer zugeordnet sind. Im Normalfall zeigt der Task-Manager nur die Prozesse des aktuellen Benutzers an. Markieren Sie PROZESSE ALLER BENUTZER ANZEIGEN, um sämtliche Prozesse des Systems anzuzeigen (Abbildung 12.9). Beachten Sie, dass der Benutzername einiger Prozesse `LOKALER DIENST` oder `NETZWERKDIENST` lautet. Wie Sie sich denken können, handelt es sich dabei um Dienste!

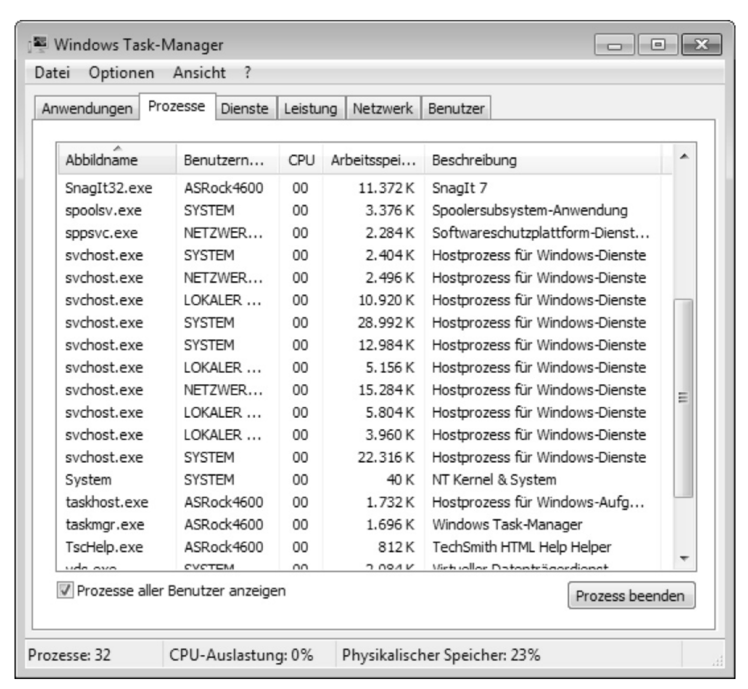


Abb. 12.9: Prozesse aller Benutzer in Windows 7

Nun kennen Sie die Grundlagen und wir wollen uns ansehen, was der Task-Manager sonst noch kann. Wenn Sie einen Prozess mit der rechten Maustaste anklicken und PROZESS BEENDEN wählen, wird dieser Prozess augenblicklich beendet. Handelt es sich bei dem Prozess um eine Anwendung, wird diese geschlossen.

Tipp: Anwendungen beenden

Starten Sie zunächst das Programm NOTEPAD und öffnen Sie dann den Task-Manager. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie ZU PROZESS WECHSELN, um weitere Informationen anzuzeigen. Wählen Sie im Kontextmenü PROZESS BEENDEN, um die Anwendung zu schließen.

Das Beenden von Prozessen ist natürlich von großer Bedeutung, aber es gibt noch mehr. Wenn Sie einen Prozess mit der rechten Maustaste anklicken, werden Ihnen verschiedene Optionen angeboten. Falls Sie einen Prozess auswählen, bei dem es sich um eine Anwendung handelt (der Name ist hier ein guter Hinweis; `winword.exe` ist z.B. Microsoft Word), wird Ihnen ein Kontextmenü wie in Abbildung 12.10 angezeigt.

Die Auswahl von DATEIPFAD ÖFFNEN führt Sie geradewegs dorthin, wo sich die entsprechende Datei befindet. Das ist besonders hilfreich, wenn Sie irgendeinen ominösen Prozess beobachten und herauszufinden versuchen, was dieser Prozess auf Ihrem Computer verloren hat.

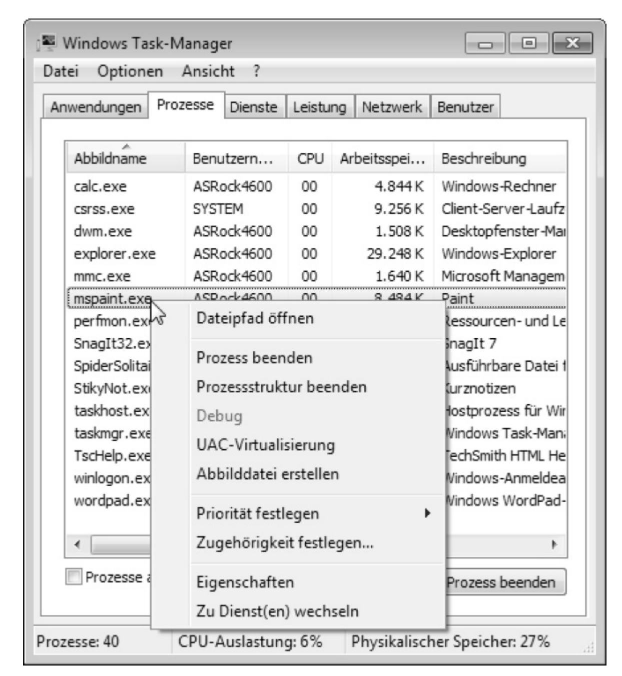


Abb. 12.10: Rechtsklick auf einen Prozess

Was PROZESS BEENDEN bewirkt, wissen Sie bereits. PROZESSSTRUKTUR BEENDEN ist besonders wichtig, aber entsprechend komplex; wir betrachten es später eingehender.

DEBUG ist deaktiviert, sofern auf Ihrem System nicht ein Windows-Debugger läuft. Siehe auch die Erklärung zu ABBILDDATEI ERSTELLEN weiter unten.

Unter Windows 7 ermöglicht UAC-VIRTUALISIERUNG älteren Programmen, die nicht dafür ausgelegt sind, den Zugriff auf geschützte Ordner zu vermeiden, Zugang zu einem »pseudogeschützten« Ordner. Für gewöhnlich handhabt Windows das automatisch, aber in seltenen Fällen kann es notwendig sein, hier Hand anzulegen. Allerdings werden Sie das kaum von sich aus tun, sondern vielmehr unter Anleitung des Supporttechnikers irgendeines Softwareherstellers, der Ihnen dann schon mitteilt, wie die UAC-Virtualisierung zu verwenden ist.

ABBILDDATEI ERSTELLEN erzeugt eine Datei mit Informationen über den Zustand des Programms in dem Moment, wo Sie diesen Punkt des Kontextmenüs anklicken. Programmierer verwenden spezielle Werkzeuge zum Debuggen um diese Dateien zu analysieren, wenn ein Programm Probleme bereitet. Normalerweise werden Sie diese Option nur dann verwenden, wenn Sie Schwierigkeiten mit einem Programm haben und der Support des Herstellers Sie darum bittet.

PRIORITÄT FESTLEGEN erlaubt es Ihnen, einem Prozess mehr oder weniger Rechenzeit zuzuteilen (Abbildung 12.11). Das ist nützlich, wenn ein bestimmter Prozess Ihren Rechner ausbremst, oder falls ein Prozess zu langsam läuft und Sie ihn beschleunigen möchten.

Das Herumbasteln an den Prozessprioritäten kann allerdings schnell ziemlich kompliziert werden. Am besten stellen Sie sich die Priorität als eine VIP-Warteschlange vor einem Fahrgeschäft in einem Vergnügungspark vor. Durch den VIP-Ausweis wird die Fahrt selbst nicht beschleunigt und »schneller anstellen« funktioniert auch nicht. Der VIP-Ausweis senkt lediglich die Anzahl der Leute, die in der Warteschlange vor Ihnen stehen. Aber was geschieht, wenn so viele Leute in der VIP-Warteschlange stehen, dass die Schlange der Leute ohne VIP-Ausweis so gut wie gar nicht mehr vorrückt?

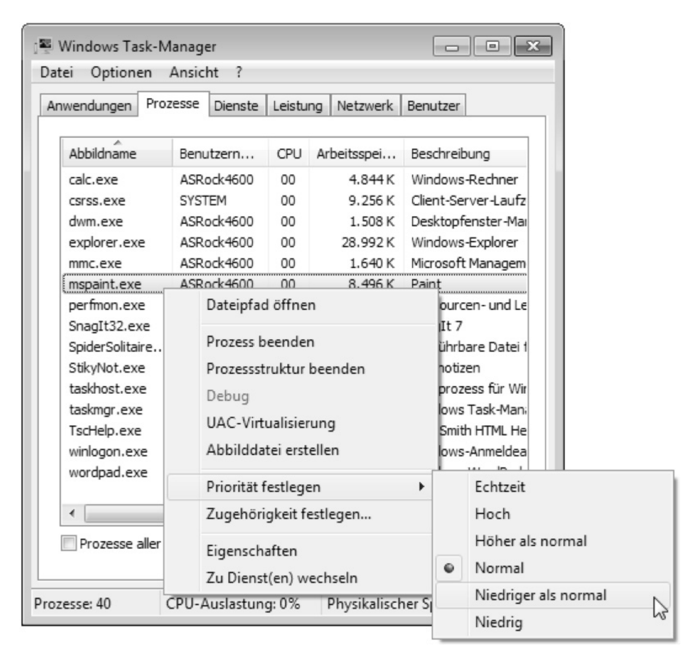


Abb. 12.11: Prozessprioritäten

Nehmen wir an, Sie möchten Ihren PC ein Video berechnen lassen. Nachdem Sie den Prozess gestartet haben, stellen Sie fest, dass die Ausgabe etwa sechs Stunden dauern wird. Außerdem gibt es beim Abspielen von Musik nun dauernd Aussetzer. Die Berechnung des Videos mag ja vielleicht wichtiger sein, aber ohne Ihre Musik können Sie nicht vernünftig arbeiten. In diesem Fall ist es am besten, entweder die Priorität eines einzelnen Prozesses zu erhöhen, der normal ablaufen soll, wie hier die Audiowiedergabe, oder aber die Priorität eines weniger zeitkritischen Prozesses (die Videoausgabe) zu senken. Alle anderen Prioritäten bleiben unangetastet. Es ist vermutlich besser, wenn Ihr System dann acht Stunden für die Videoausgabe benötigt, Sie währenddessen aber damit weiterarbeiten können, als sechs Stunden lang darauf zu verzichten.

Hinweis

Wenn Sie auch nur einem Prozess die Priorität ECHTZEIT zuweisen, kann das bereits zu einem System im Schneckentempo führen, da andere Prozesse kaum noch Rechenzeit erhalten. Vermeiden Sie die Priorität ECHTZEIT, falls möglich.

Mit ZUGEHÖRIGKEIT FESTLEGEN können Sie angeben, auf welchen CPU-Kernen ein Prozess ausgeführt werden soll. Sie werden diese Funktion kaum benötigen, es sei denn, sie starten Prozesse (etwa ältere Programme, die nicht an Mehrkernprozessoren angepasst sind), die von anderen Prozessen getrennt ausgeführt werden sollen (Abbildung 12.12).

Der Punkt EIGENSCHAFTEN bietet wenig Neues. Sie könnten ebenso gut im Windows-Explorer (Windows 7) mit der rechten Maustaste auf die ausführbare Datei klicken und EIGENSCHAFTEN wählen. Über den Punkt ZU DIENST(EN) WECHSELN gelangen Sie auf die Registerkarte DIENSTE des Task-Managers, wo Ihnen eine vollständige Liste aller dem Prozess zugehörigen Dienste präsentiert wird. Je nach Prozess sind das gar keine, einer oder mehrere. Hilfreich ist dieser Punkt des Kontextmenüs, wenn Sie Fehlermeldungen der Art »Programm konnte nicht gestartet werden, weil zugehörige Dienste nicht laufen« erhalten. Abbildung 12.13 zeigt nach Auswahl von ZU DIENST(EN) WECHSELN die Dienste an, die zum Prozess mit der PID 804 gehören.

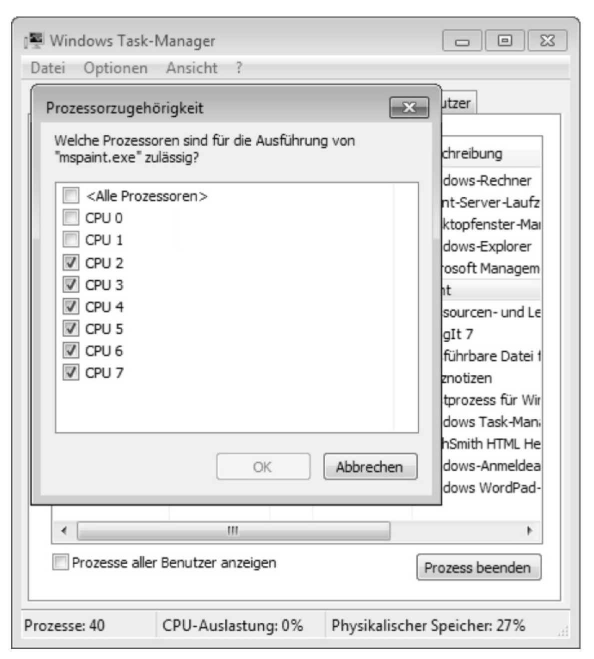


Abb. 12.12: Festlegen der Zugehörigkeit

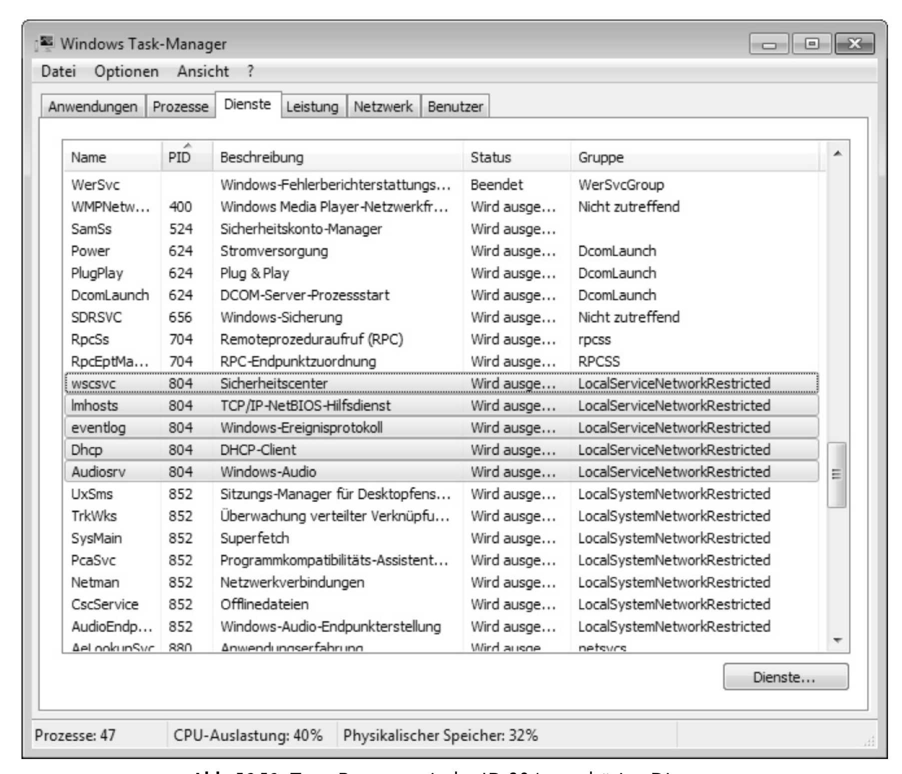


Abb. 12.13: Zum Prozess mit der ID 804 zugehörige Dienste

Zurück zum Menüpunkt PROZESSSTRUKTUR BEENDEN. Es ist durchaus üblich, dass ein einzelner Prozess von anderen Prozessen abhängt (oder andere Prozesse startet, die dann von ihm abhängen). Dadurch entsteht eine Abhängigkeitsstruktur. Der Task-Manager zeigt jedoch leider nicht an, auf welche Art und Weise die Prozesse voneinander abhängen. Dennoch gibt es die Möglichkeit, die Prozessstruktur zu beenden, wobei nicht nur der ausgewählte Prozess beendet wird, sondern auch alle Prozesse, von denen er abhängt. Das wirkt auf den ersten Blick beängstigend, da viele Prozesse von einem einzigen wichtigen Prozess abhängen. Microsoft entschärft diese Situation dadurch, dass das Beenden der Prozessstruktur der wichtigsten Systemprozesse nicht erlaubt ist.

Dessen ungeachtet wäre es schön, diejenigen Prozesse tatsächlich angezeigt zu bekommen, die man gerade abzuschießen im Begriff ist. Erfreulicherweise gibt es zu diesem Zweck den beliebten (und kostenlosen) *Process Explorer* von Mark Russinovitch (Abbildung 12.14).

Abb. 12.14: Process Explorer

Sie können sich den Process Explorer als einen gedopten Task-Manager vorstellen. Er ist sehr leistungsfähig und viele Techniker verwenden ihn anstelle des Task-Managers. Er ist zwar kein Bestandteil der CompTIA A+-Prüfungen, sollte es aber sein. Anstatt die Prozesse einfach nur der Reihe nach aufzulisten, zeigt der Process Explorer eine Baumstruktur an, in der alle Abhängigkeiten erkennbar sind.

Hinweis

Der Process Explorer kann einiges mehr, als nur eine Baumstruktur der Prozesse anzuzeigen. Laden Sie sich eine Kopie davon herunter und probieren Sie ihn aus. Sie werden schnell verstehen, warum er so außerordentlich beliebt ist. Sie finden den Process Explorer auf der Sysinternals-Website unter `https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer`.

Dienste Verwenden Sie die Registerkarte DIENSTE im Task-Manager, um direkt auf Dienste zuzugreifen (Abbildung 12.15). Hier können Dienste gestoppt oder gestartet werden. Außerdem gelangen Sie über diese Registerkarte zu den zugehörigen Prozessen eines Dienstes.

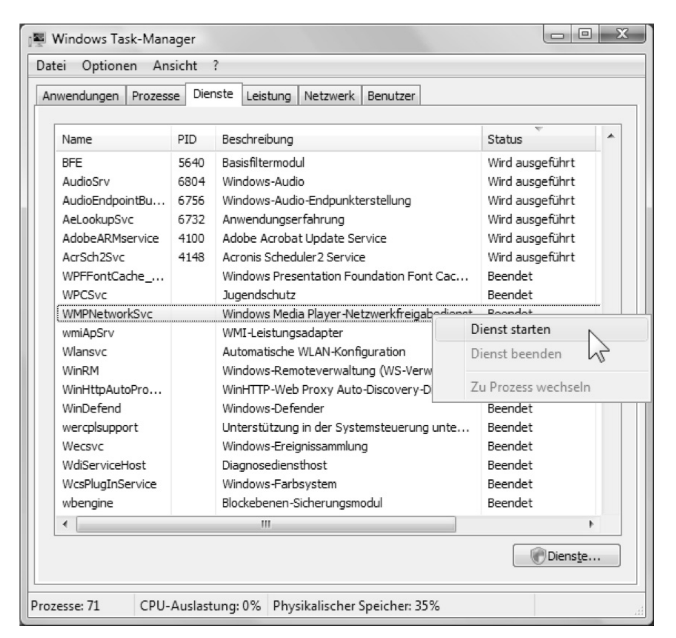


Abb. 12.15: Registerkarte DIENSTE im Task-Manager

Zur Anzeige der Dienste in Aktion können Sie auf die Schaltfläche DIENSTE im unteren Bereich der Registerkarte im Task-Manager klicken, oder in der Systemsteuerung das Applet VERWALTUNG| DIENSTE öffnen. Abbildung 12.16 zeigt das Applet in Windows 7.

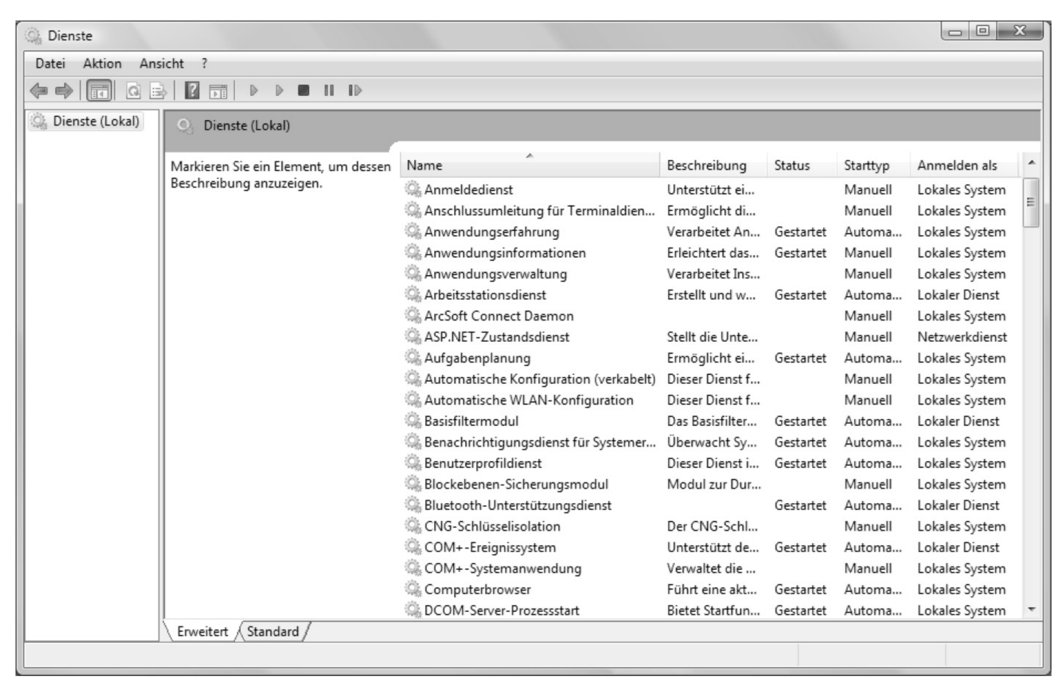


Abb. 12.16: Das Applet DIENSTE

Wichtig

Sie können das Applet DIENSTE auch durch die Eingabe von `services.msc` in das Suchfeld im Startmenü und Drücken von ↵ öffnen.

Sehen Sie sich Abbildung 12.16 etwas genauer an. Hier repräsentiert jede Zeile einen Dienst. Dienste besitzen keine eigenen Fenster, daher werden Sie über dieses Applet gestartet, gestoppt und konfiguriert. In der Spalte STATUS wird angezeigt, ob ein Dienst gerade arbeitet. Zum Konfigurieren eines Dienstes können Sie mit der rechten Maustaste auf den Namen eines Dienstes klicken. Das Kontextmenü erlaubt das Starten, Beenden, Anhalten, Fortsetzen und Neustarten eines Dienstes. Ein Klick auf EIGENSCHAFTEN zeigt ein Dialogfeld wie in Abbildung 12.17 an.

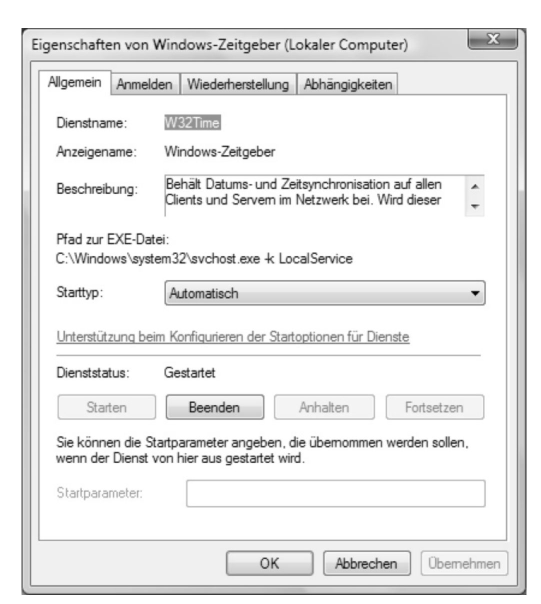


Abb. 12.17: Dialogfeld mit den Eigenschaften eines Dienstes

Von den vier Registerkarten dieses Dialogfelds werden ALLGEMEIN und WIEDERHERSTELLUNG mit Abstand am häufigsten benötigt. Auf der Registerkarte ALLGEMEIN sind Name und Beschreibung des Dienstes angegeben und Sie können den Dienst STARTEN, BEENDEN, ANHALTEN oder FORTSETZEN. Sie können außerdem festlegen, wie der Dienst gestartet wird: MANUELL (dann starten Sie ihn hier oder über das Kontextmenü), AUTOMATISCH (der Dienst startet, wenn Windows hochfährt), DEAKTIVIERT (der Dienst wird gar nicht gestartet), oder AUTOMATISCH (VERZÖGERTER START), was den Dienst nach dem Hochfahren von Windows startet, jedoch erst nachdem die anderen Dienste gestartet wurden.

Wichtig

Sie können einen Dienst über die Eingabeaufforderungen starten oder beenden, indem Sie `net start <Dienstname>` oder `net stop <Dienstname>` eingeben.

Leistung Für Optimierungszwecke ist der Task-Manager ein großartiges Werkzeug, mit dem sich feststellen lässt, wie weit und warum RAM und CPU ausgelastet sind. Auf der Registerkarte LEISTUNG finden Sie die praktisch nützlichsten Informationen: CPU-Auslastung, Verfügbarer physischer Spei-

cher, Größe des Festplatten-Caches sowie weitere Einzelheiten über Arbeitsspeicher und Prozesse. Abbildung 12.18 zeigt ein System mit einem Zweikern-Prozessor, weshalb es auch zwei getrennte Diagramme im Bereich VERLAUF DER CPU-AUSLASTUNG GIBT. Bei einem System mit einem einzelnen Prozessorkern wird hier nur ein Diagramm angezeigt.

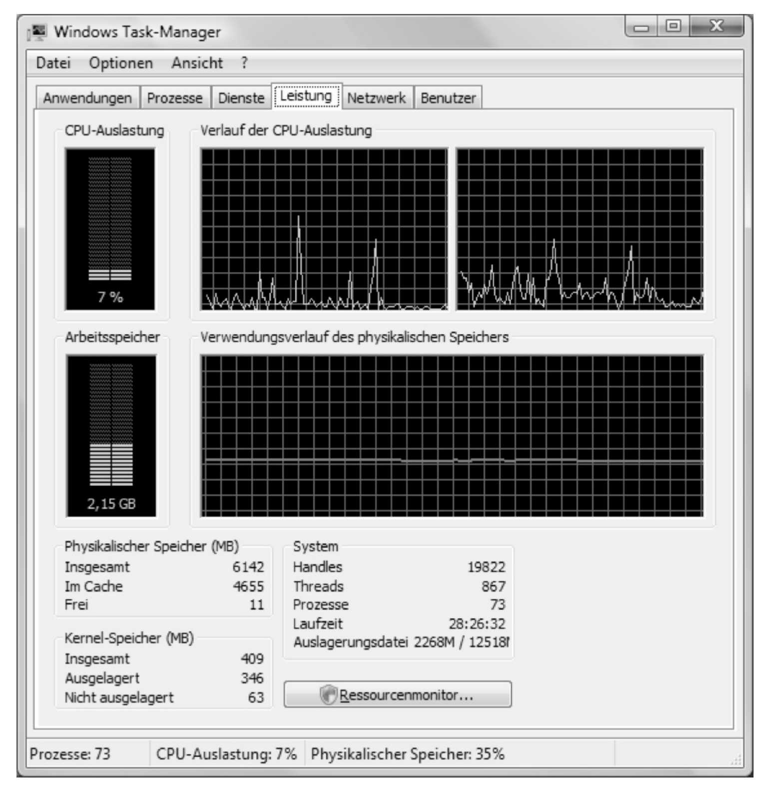


Abb. 12.18: Registerkarte LEISTUNG im Task-Manager

Beachten Sie, dass Ihnen der Task-Manager nicht nur mitteilt, wie viel CPU und RAM gerade genutzt werden, sondern auch, welches Programm diese Ressourcen nutzt. Angenommen, Ihr System läuft sehr langsam. Sie öffnen den Task-Manager und stellen fest, dass die CPU voll ausgelastet ist. Anschließend lassen Sie sich über die Registerkarte PROZESSE alle Prozesse anzeigen, die auf Ihrem System ausgeführt werden. Klicken Sie die Spalte CPU(-AUSLASTUNG) an, um die Prozesse nach der CPU-Auslastung sortieren zu lassen und um anzuzeigen, welcher die CPU besonders stark beansprucht (Abbildung 12.19)! Beenden Sie den Prozess, falls erforderlich, oder vermindern Sie seine Priorität.

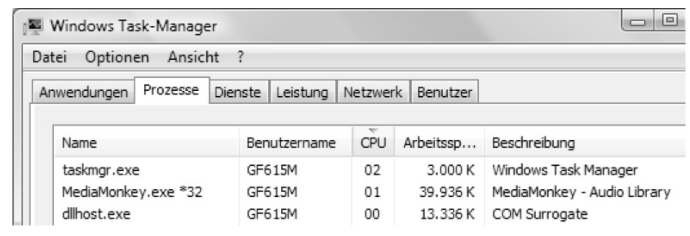


Abb. 12.19: CPU-Auslastung

Netzwerk und Benutzer Die übrigen beiden Registerkarten des Task-Managers, NETZWERK und BENUTZER, ermöglichen es Ihnen, auf einen Blick die Netzwerkauslastung zu überprüfen und anzuzeigen, welche Benutzer am lokalen System gerade angemeldet sind. Wenn Sie denken, dass die Netzwerkverbindung Ihres Computers zu langsam ist, dann ist die Registerkarte NETZWERK der geeignete Ort, das zu kontrollieren. Wird nur geringe Aktivität angezeigt, können Sie zumindest ausschließen, dass Ihr Computer die Probleme verursacht und Sie müssen die Ursache woanders suchen. Die Fehlersuche bei Netzwerkproblemen wird in Kapitel 19 noch ausführlich zur Sprache kommen.

Auf der Registerkarte BENUTZER können Sie andere Benutzer vom System abmelden, um Systemressourcen freizugeben, sofern Sie über die dafür nötigen Berechtigungen verfügen. Sie können sich außerdem selbst abmelden. Wenn ein anderer angemeldeter Benutzer eine wichtige Datei geöffnet hat, auf die Sie unbedingt zugreifen müssen, können Sie den Benutzer abmelden und damit auch die Anwendung, mit der die Datei geöffnet wurde, beenden. Nun können Sie auf die Datei zugreifen. Hierbei gehen ungesicherte Änderungen des anderen Benutzers natürlich verloren, also verwenden Sie diese Funktion mit Bedacht.

Der Task-Manager in Windows 8/8.1/10

Sie haben nun einiges über den Task-Manager in den Zeiten vor Windows 8 erfahren. Sehen wir uns also nun die Aktualisierungen an, die er erlebt hat! Manches hat sich geändert und wurde verbessert. Im neuen Task-Manager gibt es jetzt eine Ansicht WENIGER DETAILS (Abbildung 12.20), mit einer wirklich einfachen Bedienoberfläche zur Anzeige und zum Beenden laufender Programme. Für manche Benutzer ist das ausreichend – und Ihnen als Techniker dürfte klar sein, dass nicht allen Benutzern die Ansicht MEHR DETAILS angezeigt wird, wenn Sie den Task-Manager öffnen. Nach dem Umschalten auf die Ansicht MEHR DETAILS, sieht der Task-Manager schon viel vertrauter aus, aber lassen Sie sich davon nicht täuschen – viele Dinge haben sich geändert. Sehen wir uns also die größten Neuerungen an.

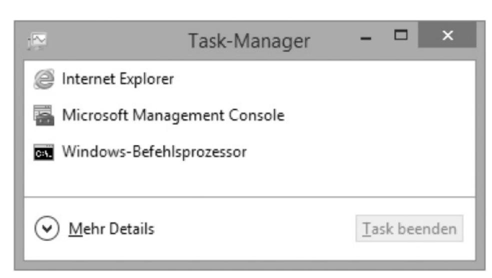


Abb. 12.20: Die Ansicht WENIGER DETAILS im Task-Manager von Windows 8.1

Wichtig

Zum Öffnen des Task-Managers können Sie nach wie vor die Tastenkombination [Strg] + [⇧] + [ESC] verwenden. Sie können aber auch mit der rechten Maustaste auf START klicken und im Kontextmenü TASK-MANAGER auswählen.

Der neue Task-Manager zeigt nach dem Öffnen nicht mehr die einfache Registerkarte ANWENDUNGEN an, sondern die Registerkarte PROZESSE, bei der sich vieles verändert hat. Die Registerkarten LEISTUNG, DIENSTE und BENUTZER sind noch vorhanden, die Inhalte der Registerkarte NETZWERK hingegen sind nun (zusammen mit weiteren neuen Informationen) Bestandteil der Registerkarte LEISTUNG. Und zu guter Letzt gibt es jetzt drei neue Registerkarten: APP-VERLAUF, AUTOSTART und DETAILS. Darüber hinaus gibt es spürbare Verbesserungen bei der Bedienung, wie z.B. die Möglichkeit, einfach mit der rechten Maustaste auf eine Spaltenüberschrift zu klicken, um die angezeigten Spalten auszuwählen (zumindest auf den meisten Registerkarten). Außerdem gibt es nun die Option ONLINE SUCHEN, wenn man einen Dienst oder einen Prozess mit der rechten Maustaste anklickt. Sehen wir uns die Registerkarten der Reihe nach etwas genauer an.

Abb. 12.21: Die Registerkarte PROZESSE im Task-Manager von Windows 10

Prozesse Vielleicht ist Ihnen aufgefallen, dass die eben erwähnte Ansicht WENIGER DETAILS große Ähnlichkeit mit einer vereinfachten Version der Registerkarte ANWENDUNGEN des alten Task-Managers aufweist. Die übrigen Bestandteile der ehemaligen Registerkarte ANWENDUNGEN sind nun mehr oder weniger Teil der Registerkarte PROZESSE. Wenn Sie in der Ansicht MEHR DETAILS den Menüpunkt ANSICHT|NACH TYP GRUPPIEREN wählen, werden die Prozesse in drei Kategorien aufgeteilt: APPS, HINTERGRUNDPROZESSE und WINDOWS-PROZESSE.

Hinweis

Diese drei Kategorien werden nur angezeigt, wenn die Prozesse nach Namen sortiert sind. Anderenfalls zeigt der Task-Manager lediglich eine Liste der laufenden Prozesse an.

Neben der Umorganisierung der Registerkarte PROZESSE hat sich auch die Philosophie geändert, was die Registerkarte eigentlich aussagen soll. Vor Windows 8 zeigte sie Name, Benutzer, CPU-Auslastung und belegten Arbeitsspeicher sowie eine Beschreibung des Prozesses an. (Keine Sorge, diese Angaben finden sich nun auf der Registerkarte DETAILS, zu der ich gleich komme.) Nun werden standardmäßig eine Beschreibung des Prozesses, dessen Status und dessen Ressourcennutzung angezeigt, inklusive CPU-Auslastung, belegtem Arbeitsspeicher, sowie Datenträger- und Netzwerkzugriff. Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, um die angezeigten Spalten auszuwählen. Es gibt jetzt die Spalten GPU und GPU-MODUL, die Auslastung und Nutzungsart der GPU anzeigen, sowie STROMVERBRAUCH und STROMVERBRAUCH (TREND), die angeben, wie viel Energie Prozesse verbrauchen (Abbildung 12.22). Die Ressourcenwerte sind farbcodiert, damit Sie Probleme auf einen Blick erkennen können.

Der Task-Manager erledigt die Anzeige mehrerer Instanzen einer Anwendung gut. Nicht nur die angezeigten Informationen haben sich geändert, auch das Kontextmenü setzt andere Schwerpunkte (Abbildung 12.23). Die meisten der erweiterten Optionen (PROZESSSTRUKTUR BEENDEN, UAC-VIRTUALISIERUNG, PRIORITÄT FESTLEGEN, ZUGEHÖRIGKEIT FESTLEGEN, ZU DIENST(EN) WECHSELN) sind ebenfalls in das Kontextmenü der Registerkarte DETAILS gewandert. Sie wurden ersetzt durch einfachere Optionen.

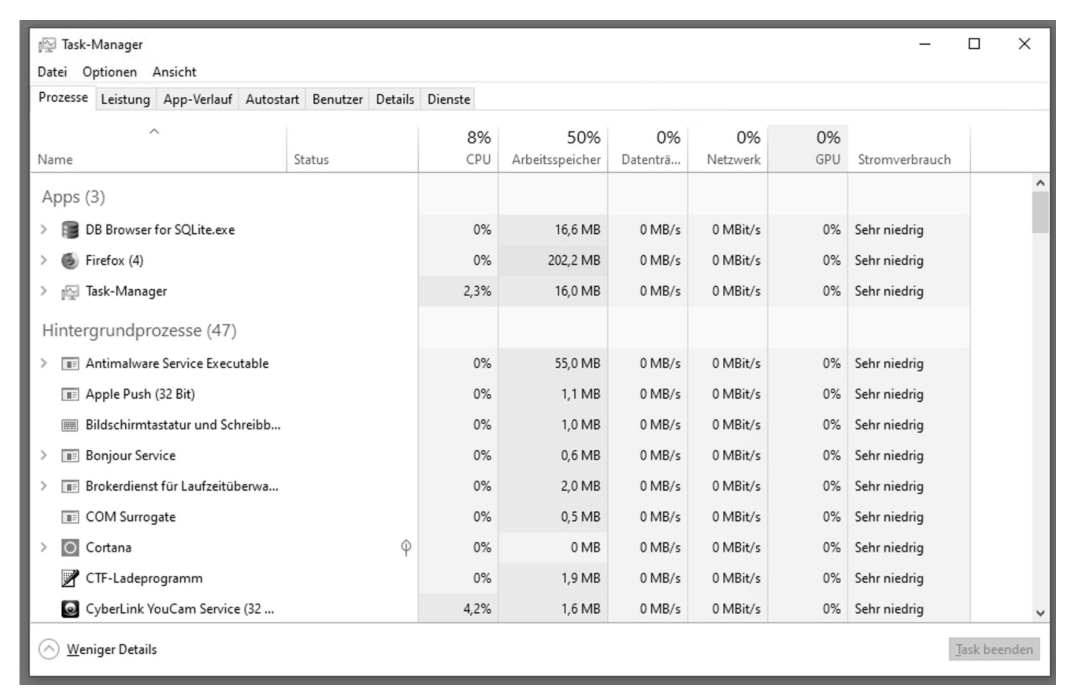


Abb. 12.22: Die Spalten GPU und Stromverbrauch

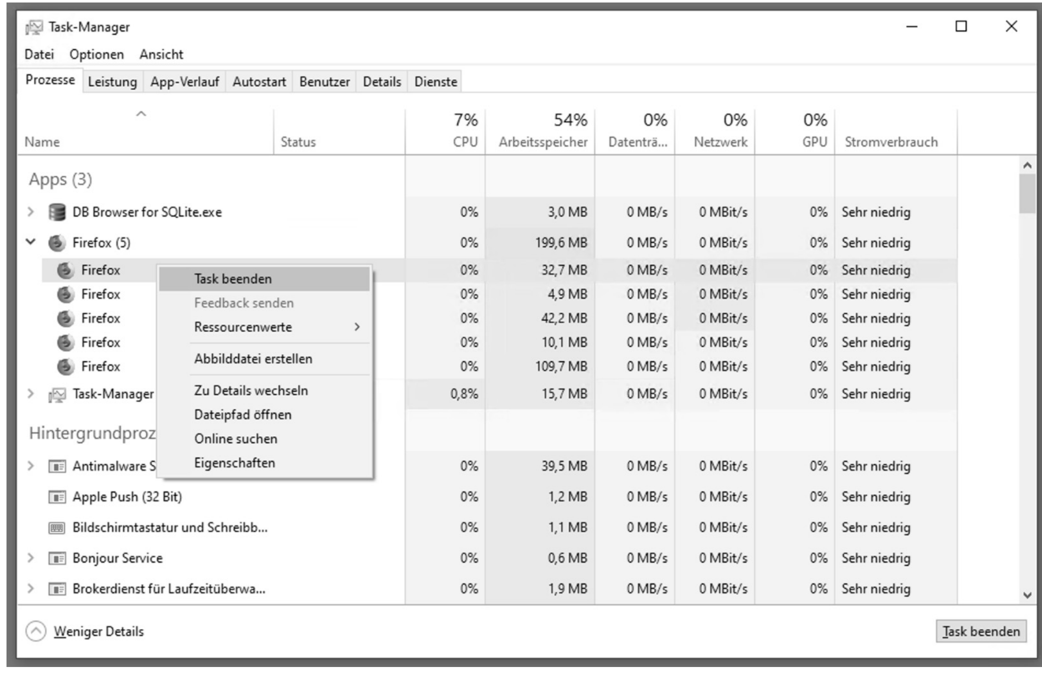


Abb. 12.23: Kontextmenü der Registerkarte PROZESSE in Windows

Klicken Sie mit der rechten Maustaste auf einen Prozess und wählen Sie im Kontextmenü TASK BEENDEN, um ihn zu schließen. Beachten Sie, dass sich diese Option von derjenigen in Windows 7 unterscheidet. Die Optionen PROZESS BEENDEN und PROZESSSTRUKTUR BEENDEN finden sich unter Windows 8/8.1/10 im Ressourcenmonitor, zu dem wir gleich kommen.

Leistung Der Sinn der Registerkarte LEISTUNG hat sich gegenüber der früheren Version des Task-Managers nicht geändert (Abbildung 12.24). Die aktualisierte Version gefällt optisch und erledigt ihre Aufgabe auch um einiges besser. Der Inhalt der ehemaligen Registerkarte NETZWERK hat hier ein neues Zuhause gefunden und außerdem wurde eine Anzeige der Festplattenzugriffe hinzugefügt. Damit gibt es nun einen Ort, an dem Sie sich alle wesentlichen Leistungskennzahlen gleichzeitig anzeigen lassen können: Auslastung von CPU und Arbeitsspeicher sowie Zugriffe auf Laufwerke und Netzwerk und in Windows 10 auch die Nutzung der GPU, falls vorhanden.

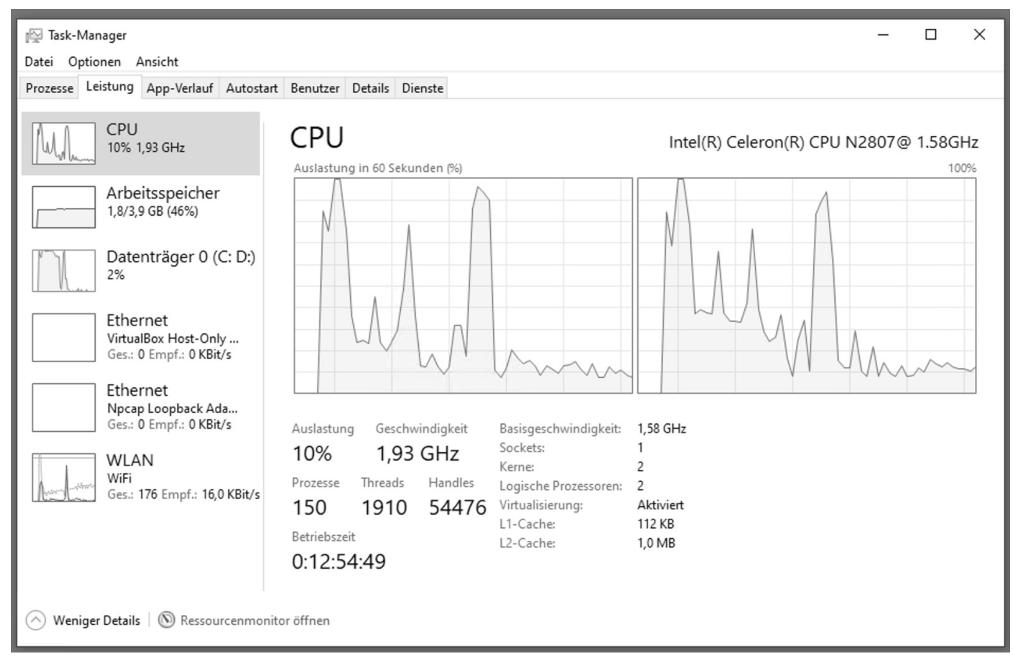


Abb. 12.24: Registerkarte LEISTUNG in Windows

Hinweis

Die Registerkarte LEISTUNG zeigt standardmäßig ein Diagramm der Gesamtauslastung der CPU an. Klicken Sie mit der rechten Maustaste auf das Diagramm und wählen Sie im Kontextmenü GRAPH ÄNDERN IN|LOGISCHE PROZESSOREN, um Diagramme der einzelnen Prozessoren anzuzeigen.

App-Verlauf Wenn man versucht, ressourcenhungrige Programme zu identifizieren, ist die aktuelle Ressourcennutzung eines Programms weniger von Bedeutung als deren zeitlicher Verlauf. Der neue Task-Manager besitzt eine Registerkarte namens APP-VERLAUF (Abbildung 12.25), die statistische Daten über CPU-Nutzung und Netzwerkzugriffe sammelt. Wenn Sie sich die Liste nach Auswahl der Registerkarte APP-VERLAUF erstmals ansehen, werden Sie feststellen, dass nicht alle Prozesse aufgeführt sind. Wählen Sie den Menüpunkt OPTIONEN|VERLAUF FÜR ALLE PROZESSE ANZEIGEN, um eine vollständigere Liste anzuzeigen. Über der Liste ist angegeben, seit wann die Ressourcenauslastung aufgezeichnet wird und Sie haben die Möglichkeit, die aktuellen Daten zu löschen, indem Sie auf AUSLASTUNGSVERLAUF LÖSCHEN klicken.

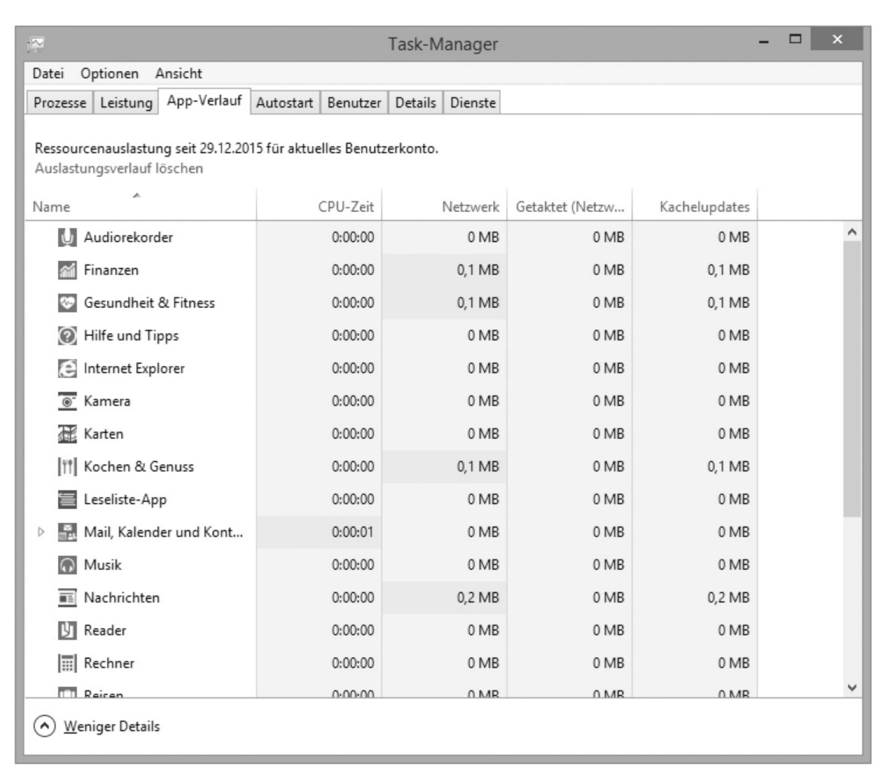


Abb. 12.25: Registerkarte APP-VERLAUF im Task-Manager von Windows

Autostart Wenn Sie Windows schon länger benutzen, wird Ihnen unweigerlich irgendein unerwünschtes Programm begegnet sein, das bei jedem Systemstart automatisch geöffnet wurde. Vielleicht haben Sie sich damit begnügt, es jedes Mal zu schließen oder das Programm sogar komplett deinstalliert. Sie hätten aber auch die Registerkarte START in einem Werkzeug namens `msconfig` verwenden können, um anzugeben, welche Programme beim Start von Windows nicht ausgeführt werden sollen. Seit Windows 8 hat die Registerkarte AUTOSTART (Abbildung 12.26) nun endlich ihren rechtmäßigen Platz im Task-Manager eingenommen und gestattet es Ihnen, dubiose automatisch startende Programme aufzuspüren und zu deaktivieren. Es gibt sogar eine Spalte STARTAUSWIRKUNGEN, in der angegeben ist, in welchem Maße ein Programm den Systemstart verlangsamt.

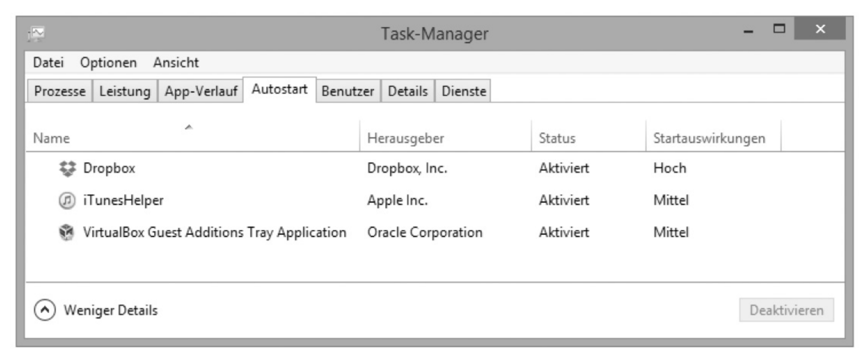


Abb. 12.26: Registerkarte AUTOSTART im Task-Manager von Windows

Benutzer Die Registerkarte BENUTZER (Abbildung 12.27) bietet im Wesentlichen dieselbe Funktionalität wie gewohnt. Hier können Sie andere Benutzer anzeigen und abmelden, es werden jedoch auch die unter einem bestimmten Benutzerkonto ausgeführten Programme angezeigt und welche Ressourcen durch sie belegt werden. Dadurch wird es vereinfacht herauszufinden, dass ein System deswegen langsam läuft, weil die Ressourcen von anderen angemeldeten Benutzern verwendet werden.

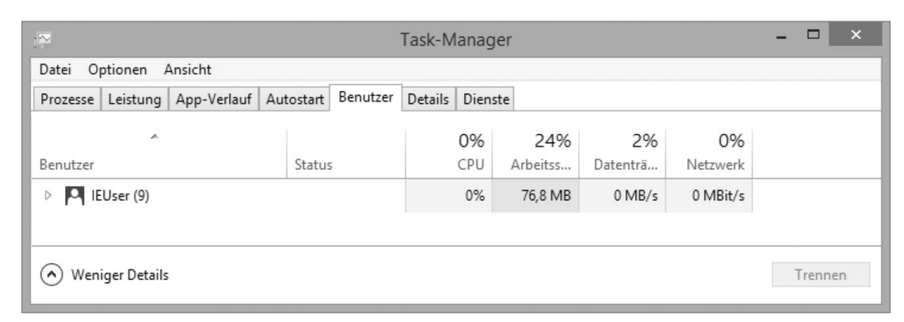


Abb. 12.27: Registerkarte BENUTZER im Task-Manager von Windows

Details Wie bereits erwähnt, hat die Registerkarte DETAILS (Abbildung 12.28) viele der Funktionalitäten übernommen, die vorher auf der Registerkarte PROZESSE zu finden waren. Hier werden die Prozesse nach Namen sortiert aufgelistet und es werden PID, Status, Benutzer, Auslastung von CPU und Arbeitsspeicher sowie eine Beschreibung angezeigt. Wenn Sie mit der rechten Maustaste auf einen Spaltenkopf klicken und im Kontextmenü auf SPALTEN AUSWÄHLEN klicken, können Sie eine schwindelerregende Anzahl von Spalten aktivieren oder deaktivieren, die Informationen über die laufenden Prozesse enthalten. Das Kontextmenü dieser Registerkarte enthält nun außerdem mit der Option WARTESCHLANGE ANALYSIEREN eine Möglichkeit, den Grund für ein eingefrorenes Programm zu ermitteln.

Task-Manager

Datei Optionen Ansicht

Prozesse Leistung App-Verlauf Autostart Benutzer Details Dienste

Name	PID	Status	Benutzername	CPU	Arbeitsspeicher (priv...	Beschreibung
AppleMobileDeviceS...	1464	Wird ausgeführt	SYSTEM	00	576 K	MobileDeviceService
csrss.exe	336	Wird ausgeführt	SYSTEM	00	504 K	Client-Server-Laufzeitpro:
csrss.exe	400	Wird ausgeführt	SYSTEM	00	624 K	Client-Server-Laufzeitpro:
Dropbox.exe	3012	Wird ausgeführt	IEUser	00	35.052 K	Dropbox
dwm.exe	716	Wird ausgeführt	DWM-1	00	10.360 K	Desktopfenster-Manager
explorer.exe	1588	Wird ausgeführt	IEUser	00	15.788 K	Windows-Explorer
iPodService.exe	3212	Wird ausgeführt	SYSTEM	00	520 K	iPodService Module (32-b
iTunesHelper.exe	2904	Wird ausgeführt	IEUser	00	700 K	iTunesHelper
Leerlaufprozess	0	Wird ausgeführt	SYSTEM	99	8 K	Zeit in Prozent, die der Pr
lsass.exe	504	Wird ausgeführt	SYSTEM	00	1.232 K	Local Security Authority P
mDNSResponder.exe	1624	Wird ausgeführt	SYSTEM	00	356 K	Bonjour Service
MsMpEng.exe	1720	Wird ausgeführt	SYSTEM	00	21.000 K	Antimalware Service Exec
NisSrv.exe	2556	Wird ausgeführt	LOCAL SERVICE	00	1.512 K	Microsoft Network Realtir
SearchIndexer.exe	2144	Wird ausgeführt	SYSTEM	00	1.576 K	Microsoft Windows Searc
services.exe	496	Wird ausgeführt	SYSTEM	00	1.020 K	Anwendung für Dienste u
smss.exe	260	Wird ausgeführt	SYSTEM	00	136 K	Windows-Sitzungs-Mana
spoolsv.exe	1208	Wird ausgeführt	SYSTEM	00	568 K	Spoolersubsystem-Anwer
svchost.exe	556	Wird ausgeführt	SYSTEM	00	1.308 K	Hostprozess für Windows
svchost.exe	600	Wird ausgeführt	NETWORK SER...	00	1.308 K	Hostprozess für Windows
svchost.exe	812	Wird ausgeführt	LOCAL SERVICE	00	5.200 K	Hostprozess für Windows

Weniger Details Task beenden

Abb. 12.28: Registerkarte DETAILS im Task-Manager von Windows

Dienste Die Registerkarte DIENSTE (Abbildung 12.29) selbst ist praktisch unverändert, wenn man von kosmetischen Aspekten absieht. Die Spalten erscheinen in derselben Reihenfolge wie früher, allerdings erscheinen nach einem Rechtsklick auf einen Dienst im Kontextmenü einige nette Änderungen zur Erleichterung der Bedienung. So kann man mit der Option ONLINE SUCHEN unbekannte Dienste erforschen und Dienste mit nur einem Klick neu starten (anstatt sie erst anzuhalten und dann wieder zu starten).

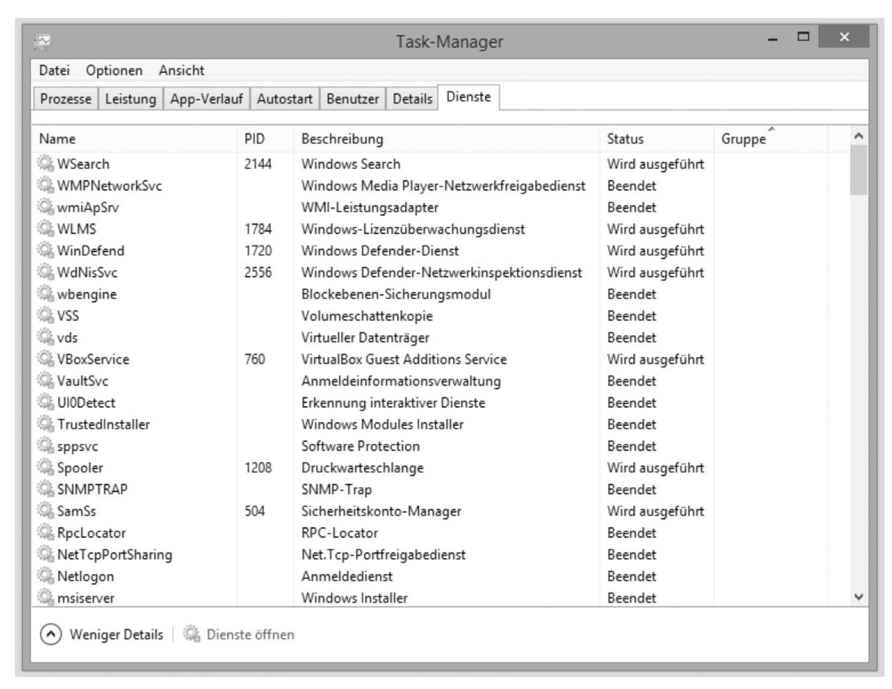


Abb. 12.29: Registerkarte DIENSTE im Task-Manager von Windows

Die Befehle tasklist und taskkill

Die beiden Kommandozeilenprogramme `tasklist` und `taskkill` ermöglichen die Verwaltung von Prozessen auf ähnliche Art, wie Sie es mit dem Task-Manager erledigen können. Mir ist kürzlich Folgendes passiert: Ich hatte die Absicht, mir die Protokolldateien eines Servers anzusehen, bei dem es einige Sicherheitsprobleme gab. Ich wollte mir also eine der Dateien mit dem Programm Notepad anzeigen lassen. Allerdings hatte ich nicht darauf geachtet, dass die Datei 300 MB groß war! Für Dateien dieser Größe ist das Programm eigentlich nicht ausgelegt und prompt fror es ein. Da ich mich ohnehin in der Eingabeaufforderung befand, entschloss ich mich, einige praktische Kommandos zu meinem Vorteil zu nutzen und mein eingefrorenes Notepad abzuschießen.

Zunächst verwendete ich den Befehl `tasklist`, der die auf einem lokalen oder entfernten Rechner laufenden Prozesse anzeigen kann. Öffnen Sie einfach die Eingabeaufforderung und geben Sie `tasklist` ein. Hier ist ein Teil der Ausgabe, die ich erhielt:

```
C:\Users\mike>tasklist
Image Name                  PID Session Name Session#  Mem Usage
===================  ====== ============ ======== ==========
System Idle Process       0 Services            0        24 K
System                    4 Services            0       940 K
smss.exe                268 Services            0       340 K
```

```
csrss.exe                372 Services            0     2,388 K
wininit.exe              444 Services            0       968 K
csrss.exe                452 Console             1     9,788 K
winlogon.exe             500 Console             1     2,420 K
services.exe             544 Services            0     4,536 K
svchost.exe              756 Services            0     4,320 K
atiesrxx.exe             904 Services            0       824 K
notepad.exe             3932 Console             0   584,868 K
```

Nachdem ich Notepads PID herausbekommen hatte, konnte ich das Programm mit dem Befehl `taskkill` beenden. Sehen Sie die speicherhungrige `notepad.exe` am Ende der Ausgabe? Sie können den Prozess unter Verwendung des Namens oder der PID beenden. Ich verwende in diesem Beispiel die PID zusammen mit dem force-Flag (`/f`), um zu gewährleisten, dass Windows Notepad auch wirklich schließt, anstatt es nur höflich aufzufordern, sich zu beenden. Das kann erforderlich sein, wenn man es mit »aufgehängten« Apps wie in diesem Fall Notepad zu tun hat.

```
C:\>taskkill /f /pid 3932
SUCCESS: The process "notepad.exe" with PID 3932 has been terminated.
```

Wichtig

In der Kommandozeilenumgebung der Windows PowerShell können Sie den Befehl `kill` verwenden, um einen laufenden Prozess zu beenden. Tatsächlich handelt es sich bei `kill` um ein Alias auf das Cmdlet `Stop-Process`, aber das brauchen Sie für die Prüfung nicht zu wissen. Kommandozeile und PowerShell werden in Kapitel 15 ausführlich behandelt.

12.3.2 Ressourcenmonitor

Der Task-Manager sollte immer die erste Wahl sein, um einen schnellen Überblick über die Auslastung des Systems zu erhalten, aber hin und wieder benötigt man mehr Details und Steuerungsmöglichkeiten. Für solche Fälle gibt es den *Ressourcenmonitor*, den Sie sich wie eine bessere Version des Task-Managers vorstellen können, die einiges mehr leistet (Abbildung 12.30).

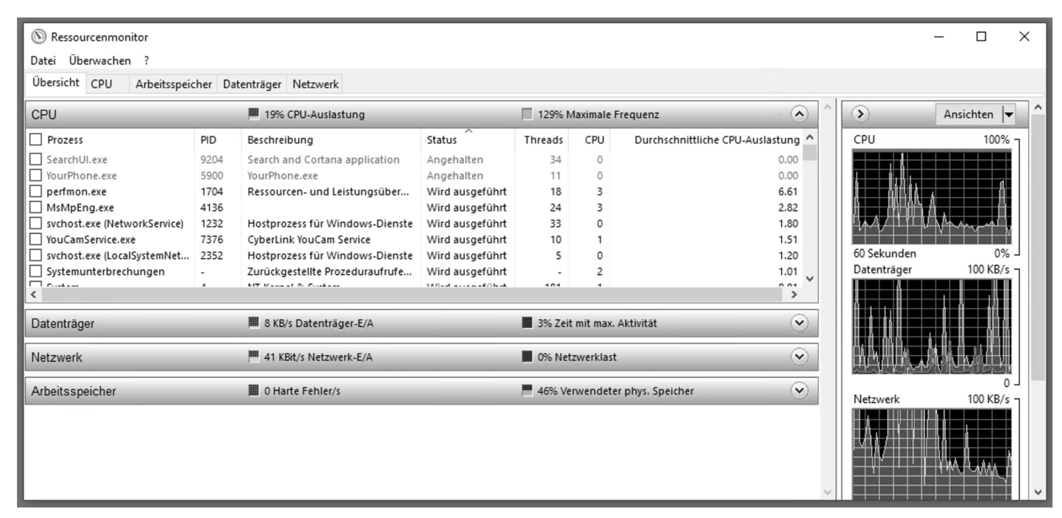


Abb. 12.30: Der Ressourcenmonitor

Sie können den Ressourcenmonitor öffnen, indem Sie auf der Registerkarte LEISTUNG im Task-Manager auf RESSOURCENMONITOR klicken. Sie finden ihn auch in der Systemsteuerung im Bereich VERWALTUNG, oder tippen Sie im Feld ZUR SUCHE TEXT HIER EINGEBEN `Ressourcenmonitor` ein. Im Ressourcenmonitor ist alles anhand der PID organisiert. Die Verwendung der PID vereinfacht die Problemdiagnose, weil sich eine vierstellige Zahl viel leichter nachverfolgen lässt als eine Textbezeichnung.

Darüber hinaus bieten Registerkarten einige interessante Features, die im Task-Manager fehlen:

- **CPU**: Ermöglicht es, einen Prozess anzuhalten, ohne ihn zu beenden.
- **Arbeitsspeicher**: Zeigt die Aufteilung des Arbeitsspeichers an.
- **Datenträger**: Zeigt die Zugriffe auf Laufwerke anhand der PID an.
- **Netzwerk**: Zeigt Netzwerkaktivität, TCP-Verbindungen und vieles mehr an.

Über die Kontextmenüeinträge PROZESS BEENDEN und PROZESSSTRUKTUR BEENDEN ermöglicht der Ressourcenmonitor, laufende Anwendungen und alle dazugehörigen Programme zu schließen. Es ist sinnvoll, diese Optionen hier unterzubringen, weil Sie im Blick haben, welche Programme beispielsweise die CPU oder das Netzwerk auslasten.

Im Allgemeinen sollten Sie den Task-Manager verwenden, wenn Sie sich einen schnellen Überblick darüber verschaffen möchten, was auf Ihrem System los ist. Falls Sie in Erfahrung bringen müssen, welcher Prozess die Ressourcen auslastet, um ihn zu beenden, dann ist der Ressourcenmonitor die richtige Wahl.

12.3.3 Leistungsüberwachung

Der Task-Manager und der Ressourcenmonitor sind gut dafür geeignet, aktuelle Probleme zu erkennen, aber was ist mit Problemen, die während Ihrer Abwesenheit auftreten? Was machen Sie, wenn Ihr System die CPU ständig zu 60 Prozent auslastet – ist das gut oder schlecht? Unter Windows gibt es Werkzeuge, die Sie zur Protokollierung der Ressourcennutzung einsetzen können, um z.B. die CPU- und RAM-Auslastung über einen längeren Zeitraum hinweg beobachten zu können. Ein guter Techniker verwendet die LEISTUNGSÜBERWACHUNG als geeignetes Werkzeug, um die Nutzung der Systemressourcen zu überwachen.

Sie können die LEISTUNGSÜBERWACHUNG in der Systemsteuerung über das Applet VERWALTUNG öffnen. Sie können das Tool auch über das Startmenü, Eingabe von `perfmon.msc` im Suchfeld und Drücken von [↵] starten. Dann öffnet sich ein Fenster, das Informationen über die Leistungsüberwachung und eine Systemübersicht anzeigt (Abbildung 12.31). Hier kann man allerdings nicht viel machen. Klicken Sie links auf das Icon LEISTUNGSÜBERWACHUNG, um die Überwachung in Echtzeit zu starten. Alle bisherigen Windows-Versionen verfügten in der einen oder anderen Form über ein solches Werkzeug. In den meisten Fällen kann man aber stattdessen auch den Ressourcenmonitor verwenden. Wenn man die Überwachung erstmals startet, ist das ziemlich eintönig (Abbildung 12.32). Aber wenn Sie eine bestimmte sehr detaillierte Überwachung durchführen möchten, könnten Sie durchaus einen Grund haben, das Werkzeug zu verwenden. Bevor Sie mit der Leistungsüberwachung zu arbeiten beginnen, müssen Sie die beiden Begriffe *Datenobjekt* und *Leistungsindikator* verstanden haben.

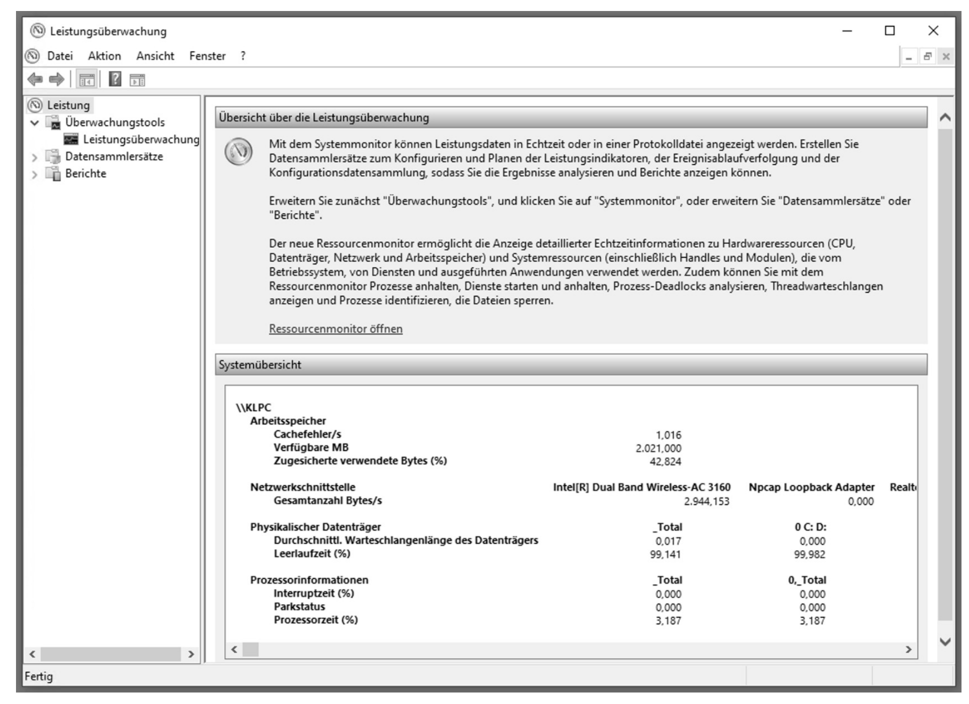


Abb. 12.31: Startbildschirm der LEISTUNGSÜBERWACHUNG

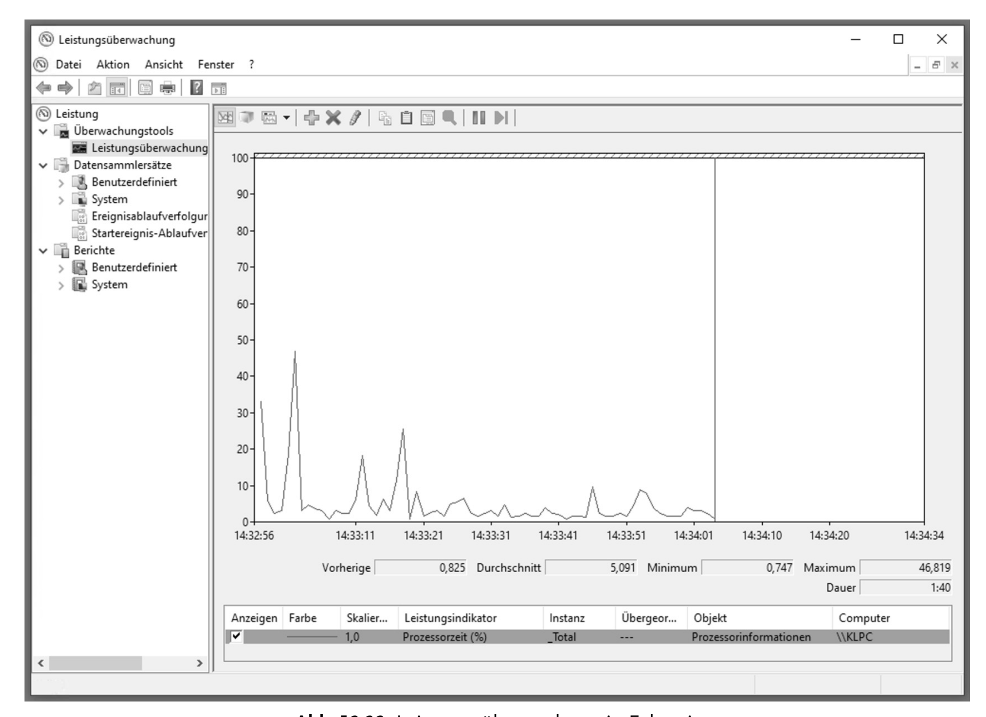


Abb. 12.32: Leistungsüberwachung in Echtzeit

Datenobjekte und Leistungsindikatoren

Für die Nützlichkeit der Leistungsüberwachung sind Datenobjekte und Leistungsindikatoren maßgeblich. Ein Datenobjekt ist eine Systemkomponente mit einem Satz von Eigenschaften, die vom Betriebssystem als Ganzes verwaltet werden kann. Ein Leistungsindikator protokolliert bestimmte Informationen über ein Objekt. Das Prozessor-Datenobjekt beispielsweise verfügt über den Leistungsindikator PROZESSORZEIT (%), der die zur Ausführung eines Threads, der sich nicht im Leerlauf befindet, benötigte Prozessorzeit in Prozentwerten misst. Einem Datenobjekt können dabei viele Leistungsindikatoren zugeordnet sein.

Leistungsüberwachung verwenden

Die Leistungsüberwachung sammelt Echtzeitdaten über Objekte wie etwa den Speicher, physische Datenträger, den Prozessor und/oder das Netzwerk und zeigt diese als Grafik in einem Liniendiagramm, einem Histogramm (Balkendiagramm) oder einem einfachen Bericht an. Wenn Sie die Leistungsüberwachung erstmals starten, werden die Daten grafisch dargestellt. Die angezeigten Daten beziehen sich auf die unter dem Diagramm angegebenen Leistungsindikatoren. Wenn Sie Leistungsindikatoren hinzufügen möchten, klicken Sie die Schaltfläche HINZUFÜGEN (mit dem Plus-Zeichen) an oder drücken zum Öffnen des Dialogfeldes LEISTUNGSINDIKATOREN HINZUFÜGEN `Strg` + `I`. In der Liste können Sie eines der zahlreichen Datenobjekte zur Überwachung auswählen. Schön am Dialogfeld LEISTUNGSINDIKATOREN HINZUFÜGEN ist, dass Sie einen Leistungsindikator auswählen und durch Aktivieren des Kontrollkästchens BESCHREIBUNG ANZEIGEN jederzeit eine Erklärung des Indikators bekommen können (Abbildung 12.33). Probieren Sie das jetzt einfach einmal aus!

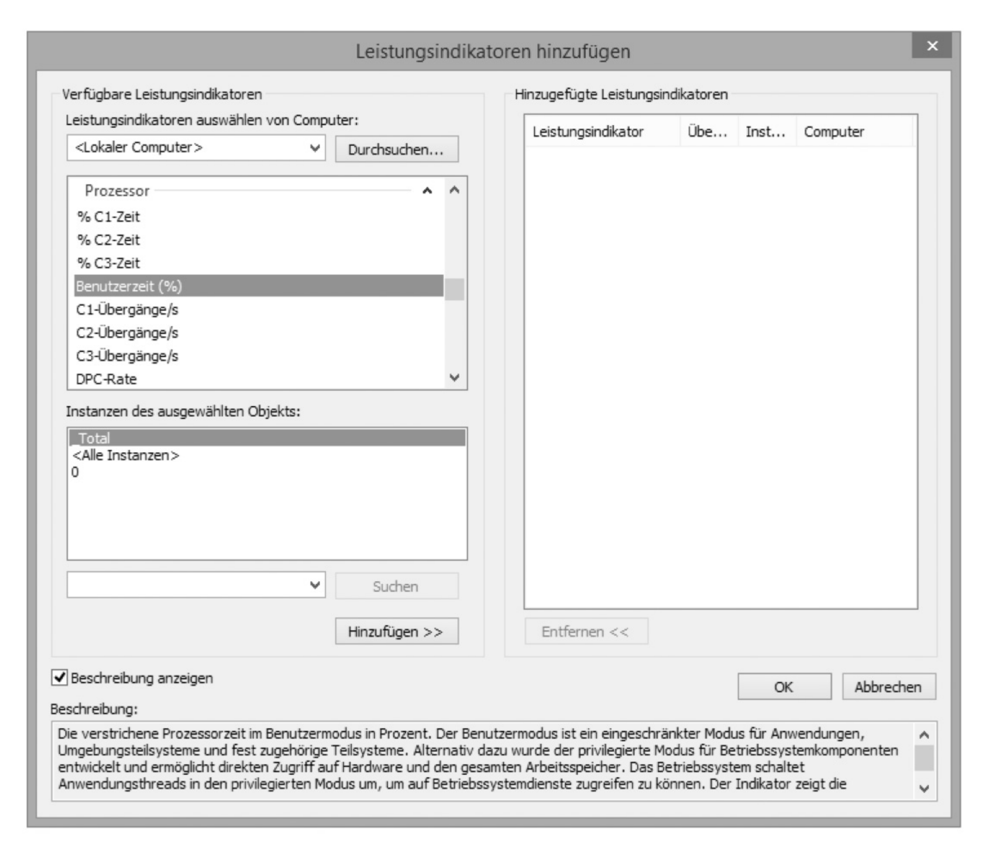


Abb. 12.33: Das Dialogfeld LEISTUNGSINDIKATOREN HINZUFÜGEN

Datensammlungssätze

Microsoft hat *Datensammlungssätze* in die Leistungsüberwachung mit aufgenommen, über die sich Indikatoren beim Erstellen von Berichten zu Gruppen zusammenfassen lassen. Sie können über die Option BENUTZERDEFINIERT eigene Datensammlungssätze erstellen oder einfach die vordefinierten Systemsätze verwenden. Wenn Sie einen Datensammlungssatz erstellt haben, können Sie die Option BERICHTE zur Anzeige der Ergebnisse nutzen (Abbildung 12.34). Über Datensammlungssätze können Sie nicht nur zu überwachende Indikatoren auswählen, sondern auch deren Überwachungszeiten planen.

Wichtig

In den CompTIA A+-Prüfungen werden Ihnen nicht allzu viele detaillierte Fragen zur Leistungsüberwachung gestellt werden. Deshalb sollten Sie dieses hervorragende Werkzeug aber nicht ignorieren! Wenn Sie die Nutzung wirklich verstanden haben, dann können Sie alle Systemereignisse überwachen und somit Probleme besser diagnostizieren.

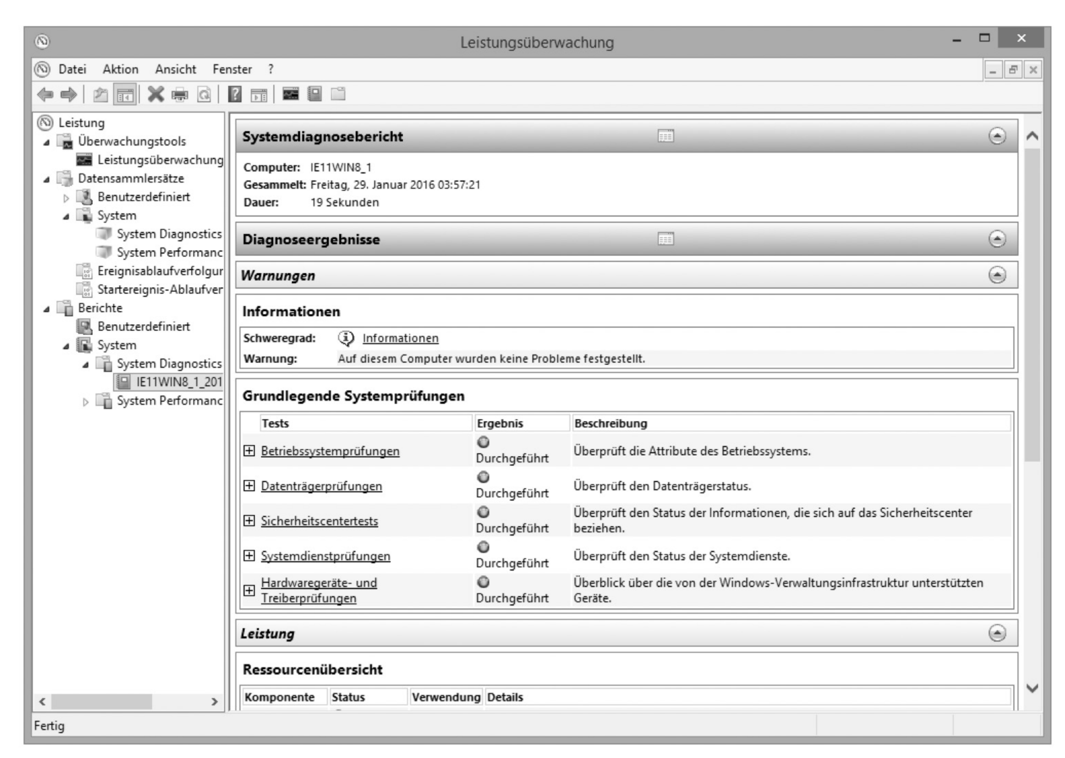


Abb. 12.34: Beispiel für einen Bericht

12.4 Werkzeuge für Programmierer

Microsoft stellt in Windows eine Reihe von Werkzeugen bereit, die weitaus mehr leisten als das, was Techniker für gewöhnlich benötigen. In der CompTIA A+-Prüfung 1002 können insbesondere die eigentlich für Programmierer gedachten Applets vorkommen, die Einfluss auf die Art der Programmierung vieler Anwendungen haben. Lesen Sie weiter, um mehr über Komponentendienste und Datenquellen (ODBC) zu erfahren. Beide Applets finden Sie in der Systemsteuerung unter VERWALTUNG.

12.4.1 Komponentendienste

Um alles zu verstehen, was mit den *Komponentendiensten* machbar ist, wäre eine enorme Informationsmenge erforderlich – weitaus mehr, als die CompTIA A+-Prüfungen umfassen. Seit es Windows gibt, hat Microsoft stets verschiedene Werkzeuge (mit Bezeichnungen wie COM, DCOM und COM+) herausgebracht, mit denen Programmierer Datenobjekte (die Bestandteile von Programmen sind) zwischen den verschiedenen Anwendungen eines einzelnen Computers austauschen konnten. Im Laufe der Zeit wurden diese Verfahren ausgebaut, damit Datenobjekte auch über ein Netzwerk ausgetauscht werden können.

In fast allen Fällen ist zur gemeinsamen Nutzung dieser Objekte nicht mehr erforderlich, als eine Anwendung zu installieren, die solche Funktionen verwendet. Die Komponentendienste stehen für die seltenen Fälle bereit, in denen entweder etwas nicht funktioniert oder aber ein Programmierer Ihre Hilfe benötigt, weil manuelle Änderungen durchgeführt werden müssen (Abbildung 12.35). In einem Unternehmen, das hauseigene oder maßgeschneiderte Anwendungsprogramme einsetzt, ist es ziemlich wahrscheinlich, dass die Komponentendienste benötigt werden, um gemeinsam mit den Programmierern die Anwendungen zu installieren und so einzurichten, dass sie wie gewünscht arbeiten. Kommerzielle Dritthersteller-Software, die Sie im Laden kaufen können, sollte während des Installationsvorgangs dafür sorgen, dass die entsprechenden Komponenten korrekt konfiguriert werden. Daher ist es so extrem selten, dass Sie sich mit den Komponentendiensten befassen müssen.

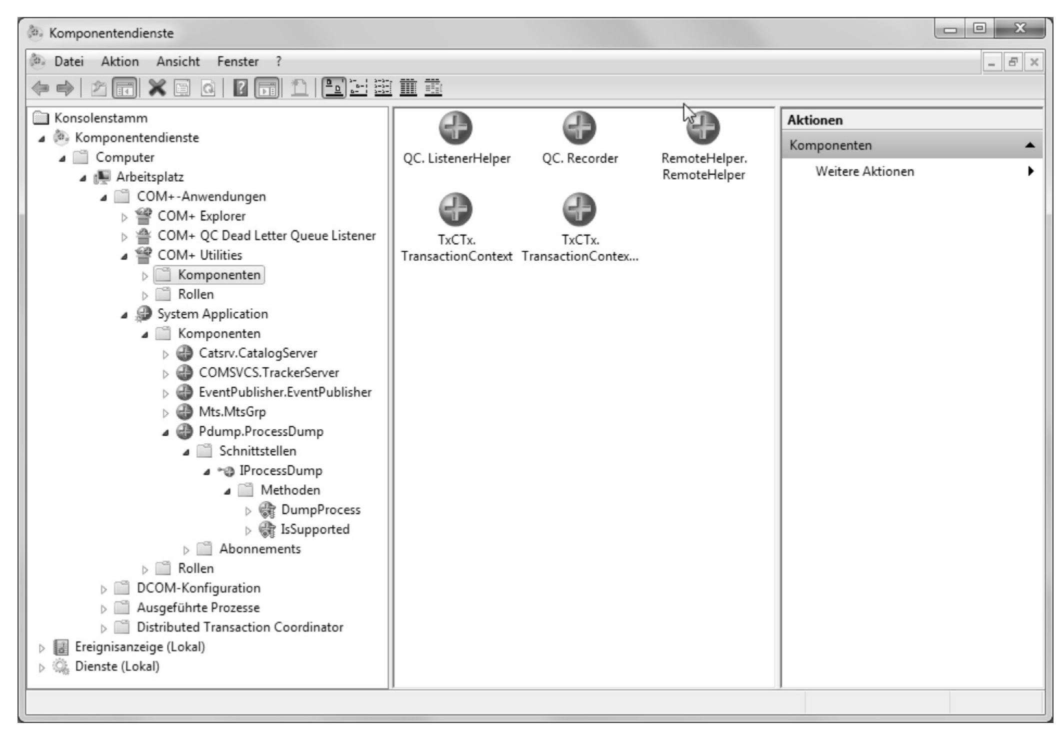


Abb. 12.35: Komponentendienste in Windows 7

12.4.2 Datenquellen

Einer der ältesten und häufigsten Gründe für die Vernetzung von Computern ist der Wunsch, gemeinsam auf eine Datenbank zuzugreifen. Auf den einzelnen Computern läuft dabei aber weder dasselbe Betriebssystem noch die gleiche Software. Hier glänzt *ODBC* (*Open Database Connectivity*) mit seinen

Fähigkeiten. ODBC ist ein Programmierstandard, der es den Softwareentwicklern erlaubt, Datenbanken und Anwendungen zu erstellen, die unabhängig von Betriebssystem und verwendetem Programm Datenbankabfragen beantworten bzw. ausführen können.

Microsofts Werkzeug zum Konfigurieren von ODBC heißt *ODBC-Datenquellen-Administrator* (ODBC Data Source Administrator) (Abbildung 12.36). Mit dem ODBC-Datenquellen-Administrator können Sie sogenannte *Datenquellennamen* (*DSN – Data Source Names*) erstellen und verwalten, mittels derer ODBC auf Datenbanken zugreifen kann. ODBC-fähige Anwendungen verwenden die Datenquellennamen, um ODBC zu befragen, wo die Datenbanken zu finden sind. Sie werden den ODBC-Datenquellen-Administrator allerdings kaum verwenden müssen, es sei denn, dass Sie selbst eine gemeinsam genutzte Datenbank erstellen wollen.



Abb. 12.36: ODBC-Datenquellen-Administrator in Windows 8.1

Die 64-Bit-Versionen von Windows bringen eine 32-Bit- und eine 64-Bit-Version des ODBC-Werkzeugs mit. Die 64-Bit-Version wird zusammen mit 64-Bit-Datenbanken verwendet, während für 32-Bit-Datenbanken die 32-Bit-Version genutzt wird.

Die gemeinsame Nutzung von Ressourcen über ein Netzwerk werden wir in Kapitel 19, *Lokale Netzwerke*, eingehend betrachten.

12.5 Wiederholung

12.5.1 Fragen

1. Wie lautet der Name des Programms, das Windows bootet?
   A. `NTFS`
   B. msconfig
   C. `bootmgr`
   D. Registry
2. Wie lautet die Bezeichnung für die Kommandozeilenversion des Task-Managers?
   A. `taskman`
   B. `tasklist`
   C. `taskkill`
   D. `tasks`

3. Welche Einstellungen dienen bei der Leistungsüberwachung dazu, die Ressourcennutzung nachzuverfolgen? (Wählen Sie zwei Antworten aus.)
   A. Prozesse
   B. Datenobjekte
   C. Leistungsindikatoren
   D. Werte
4. Was kann der Registry-Hauptschlüssel enthalten? (Wählen Sie zwei Antworten aus.)
   A. Unterschlüssel
   B. Unterordner
   C. Werte
   D. Datenobjekte
5. Welcher Registry-Hauptschlüssel enthält Informationen, die nicht benutzerspezifisch sind?
   A. `HKEY_LOCAL_MACHINE`
   B. `HKEY_USERS`
   C. `HKEY_CURRENT_USER`
   D. `HKEY_CLASSES_ROOT`
6. Welche der folgenden Aussagen über den Bootvorgang von Windows trifft zu?
   A. BIOS verwendet den `bootmgr` nicht.
   B. UEFI sucht nach dem MBR, der den Bootcode zum Start von `bootmgr` findet.
   C. BIOS sucht nach dem MBR, der den Bootcode zum Start von `bootmgr` findet.
   D. UEFI verwendet den `bootmgr` nicht.
7. Wie wird der Registrierungs-Editor von der Eingabeaufforderung aus gestartet? (Wählen Sie zwei Antworten aus.)
   A. `regedit`
   B. `reg`
   C. `regeditor`
   D. `rgstry`
8. Sven ruft an und beklagt sich darüber, dass ein bestimmtes Programm (ich nenne hier keine Namen) sich aufgehängt hat. Welches Werkzeug sollte er benutzen, um das Programm sofort zu beenden? Wie kann er das Tool öffnen?
   A. Task-Manager mit [Strg] + [⇧] + [ESC] öffnen
   B. Task-Manager mit [Strg] + [T] + [M] öffnen
   C. Leistungsüberwachung über VERWALTUNG starten
   D. Leistungsüberwachung mit [Strg] + [P] + [M] öffnen
9. Welches der folgenden Werkzeuge erlaubt es, die Ressourcennutzung anhand der PID nachzuverfolgen, anstatt eine Textbezeichnung zu verwenden?
   A. Leistungsüberwachung
   B. PID-Monitor
   C. Ressourcenmonitor
   D. Task-Manager

10. Welche Option in Windows 7 ermöglicht es, ein potenziell problematisches Programm und alle dazugehörigen Programme zu schließen?
    A. Strg + Alt + Entf
    B. Strg + Alt + ESC
    C. Rechtsklick im Task-Manager auf den Prozess und Auswahl von PROZESS BEENDEN
    D. Rechtsklick im Task-Manager auf den Prozess und Auswahl von PROZESSSTRUKTUR BEENDEN

12.5.2 Antworten

1. **C.** Windows verwendet `bootmgr` zum Booten.
2. **B.** Der Befehl `tasklist` startet die Kommandozeilenversion des Task-Managers.
3. **B, C.** Datenobjekte und Leistungsindikatoren müssen in der Leistungsüberwachung festgelegt werden, um die Ressourcennutzung zu überwachen.
4. **A, C.** Der Registrierungshauptschlüssel enthält Unterschlüssel und Werte.
5. **A.** Der Registry-Hauptschlüssel HKEY_LOCAL_MACHINE enthält Informationen, die nicht benutzerspezifisch sind.
6. **C.** Beim Start von Windows sucht das BIOS nach dem MBR, der den Bootcode zum Start des Betriebssystems findet.
7. **A.** Von der Eingabeaufforderung aus können Sie den Befehl `regedit` verwenden, um den Registrierungs-Editor zu starten.
8. **A.** Um ein Programm sofort zu beenden, benötigen Sie den Task-Manager. Am einfachsten lässt er sich mit der Tastenkombination Strg + ⇧ + ESC starten.
9. **C.** Der Ressourcenmonitor organisiert alles anhand der PID. Die Verwendung der PID vereinfacht die Problemdiagnose häufig, weil sich eine vierstellige Zahl viel leichter nachverfolgen lässt als eine Textbezeichnung.
10. **D.** Der Task-Manager in Windows 7 bietet die Option PROZESSSTRUKTUR BEENDEN, um ein Programm und alle dazugehörigen Programme zu schließen. Unter Window 8/8.1/10 finden Sie diese Option auf der Registerkarte DETAILS.

Benutzer, Gruppen und Berechtigungen 13

Themen in diesem Kapitel:

- Benutzer und Gruppen
- NTFS-Berechtigungen
- Windows-Rechner auf sichere Weise gemeinsam nutzen
- Sicherheitsrichtlinien und Benutzerkontensteuerung

Der Massenspeicher Ihres Computers enthält jede Menge Dateien, die geschützt werden müssen. Private Word-Dokumente, Tabellenkalkulationsdateien, Fotos und Videos, auf die andere nicht zugreifen sollen. Es gibt kritische Dateien, wie diejenigen, die zum Betriebssystem gehören, die nicht versehentlich gelöscht werden sollen. Es gibt einen Browser-Verlauf und Download-Ordner, die Dateien enthalten, die Sie behalten möchten und brauchen. Wie also werden diese Dateien vor anderen Benutzern geschützt, die den Computer hin und wieder ebenfalls benutzen? Die Antwort lautet: durch Benutzerkonten, Gruppen und Berechtigungen.

Windows verwendet eine Kombination von Benutzerkonten, Gruppen und NTFS-Berechtigungen, um Dateien und Ordner umfassend zu schützen. Diese Kombination von Benutzern, Gruppen und NTFS lässt sich von einzelnen Rechnern bis hin zu weltumspannenden Rechnernetzwerken skalieren.

Zum Verständnis der Sicherheitsaspekte in Windows ist es hilfreich zu betrachten, wie NTFS auf einem einzelnen, eigenständigen Rechner funktioniert, an dem sich im Laufe eines Tages mehrere Benutzer an- und abmelden. In Kapitel 19, *Lokale Netzwerke*, komme ich auf viele Themen dieses Kapitels zurück und wir werden uns ansehen, wie dieselben Werkzeuge dazu eingesetzt werden können, den Computer in einer Netzwerkumgebung zu schützen.

In diesem Kapitel befassen wir uns zunächst mit Benutzerkonten, Kennwörtern und Gruppen und wenden uns dann den feingranularen Schutzfunktionen von NTFS zu. Der dritte Abschnitt beschreibt die Methoden zur gemeinsamen Nutzung von Inhalten. Das Kapitel schließt mit einem Blick hinter die Kulissen der Sicherheitsrichtlinien und der Benutzerkontensteuerung.

1002

13.1 Authentifizierung über Benutzer und Gruppen

Grundlage der Sicherheit ist das *Benutzerkonto*, eine eindeutige Kombination von Benutzername und Kennwort, die in einer Datenbank auf Ihrem Computer gespeichert ist und dem Benutzer Zugang zum System gewährt. Normalerweise ist ein Benutzerkonto einem menschlichen Benutzer zugeordnet, es gibt aber auch Benutzerkonten, die dem System zugewiesen sind, damit es Programme ausführen kann. So gibt es beispielsweise auf jedem Windows-Computer ein SYSTEM-Benutzerkonto, das Windows benutzt, um Programme zu starten. Der Schutz Ihrer Daten basiert im Wesentlichen auf zwei Mechanismen, der Authentifizierung und der Autorisierung.

Bei der *Authentifizierung* handelt es sich um die Identifizierung eines Benutzers und die Gewährung des Zugangs. Für gewöhnlich handelt es sich um eine Person, die versucht, auf das System zuzugreifen. In Windows erfolgt die Authentifizierung zumeist über einen Benutzernamen und ein Kennwort. Bei der Anmeldung am System gibt der Benutzer seinen Benutzernamen und sein Kennwort ein.

Hinweis

Die *Authentifizierung* gewährt einem Benutzer Zugang zum System. Durch die *Autorisierung* wird festgelegt, welche Berechtigungen er besitzt.

Nachdem ein Benutzer erst einmal authentifiziert ist, muss er *autorisiert* werden. Bei der *Autorisierung* wird festgelegt, was einem Benutzer auf einem bestimmten System erlaubt bzw. untersagt ist. Die Autorisierung für den Zugriff auf Dateien und Ordnern wird vom NTFS-Dateisystem kontrolliert, das den Benutzern und Gruppen Berechtigungen zuweist. Diese Berechtigungen legen genau fest, was ein Benutzer mit den Ressourcen des Systems anstellen darf. Wir verschaffen uns zunächst einmal einen Überblick über Benutzerkonten, Kennwörter und Gruppen und betrachten anschließend die Konfiguration von Benutzern und Gruppen in Windows.

Hinweis

In diesem Kapitel werden Benutzerkonten, Kennwörter und Gruppen anhand von Windows erläutert. Ihnen sollte jedoch klar sein, dass alle anderen Betriebssysteme ausnahmslos ebenfalls Benutzerkonten, Kennwörter und Gruppen verwenden.

13.1.1 Benutzerkonten

Zu jedem Benutzerkonto gehören ein Benutzername und ein Kennwort. Der Benutzername besteht aus einer Zeichenkette, mit der sich der Benutzer gegenüber dem System identifiziert. Mögliche Benutzernamen sind beispielsweise »Mike1«, »hans.dampf« oder »irgend.jemand@sonstwo.com«. Jedem Benutzernamen ist ein Kennwort zugeordnet, ein eindeutiger Schlüssel, der nur dem System und der Person bekannt ist, die diesen Benutzernamen verwendet. Benutzername und Kennwort werden auf dem System verschlüsselt gespeichert und Zugriff wird nur gewährt, wenn bei der Anmeldung am System ein gültiger Benutzername mit dem richtigen Kennwort angegeben wird.

Alle Windows-Systeme speichern die Benutzerkontendaten in einer verschlüsselten Datenbank. In Windows wird ein einzelner Datensatz in dieser Datenbank als *lokales Benutzerkonto* bezeichnet (Abbildung 13.1).

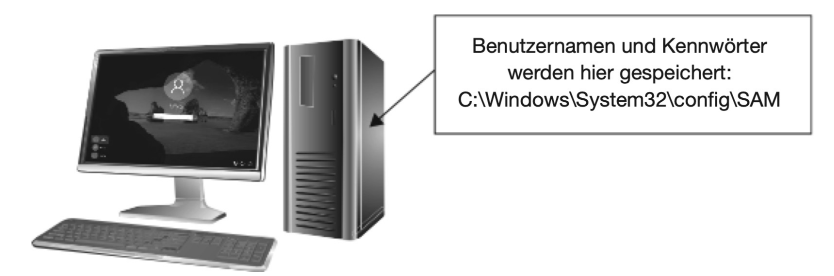


Abb. 13.1: Lokale Benutzerkonten werden auf dem System gespeichert.

Bei Benutzerkonten in Umgebungen, die ständig mit dem Internet verbunden sind, wird es schnell kompliziert. In Chrome OS kann man nur dann alle Möglichkeiten nutzen, wenn man sich mit einem Google-Konto anmeldet. Bei Linux ist das anders; hier sind lokale Benutzerkonten vorherrschend (die mit einem bestimmten Computer und Benutzer verknüpft sind). Windows und macOS unterstützen sowohl lokale Benutzerkonten als auch die Anmeldung mit einem Microsoft- oder Apple-Konto.

Sie können einen mit dem Internet verbundenen Rechner so einrichten, dass er sich mit einem globalen Benutzerkonto verbindet. Das globale Benutzerkonto funktioniert wie ein lokales, bietet jedoch den Vorteil, dass eine Synchronisierung mit bestimmten Einstellungen des globalen Benutzerkontos

stattfindet. Beispielsweise erscheint das Bild, das ich auf meinem Desktop-Rechner zu Hause als Schreibtischhintergrund verwende, auch auf meinem Laptop als Schreibtischhintergrund (wenn ich mich an beiden Geräten mit meinem Microsoft-Benutzerkonto anmelde).

Hinweis

Den Ausdruck *globales Benutzerkonto* habe ich mir ausgedacht. Die verschiedenen Unternehmen verwenden jeweils eigene Bezeichnungen, wie Microsoft-Benutzerkonto, Apple-ID oder Gmail-Konto. Sie verstehen schon, was gemeint ist.

Beim Anlegen eines (lokalen oder globalen) Benutzerkontos wird nicht nur ein Benutzername zur Datenbank hinzugefügt, es werden auch verschiedene persönliche Ordner auf dem Computer erzeugt. Windows legt beispielsweise für jeden Benutzer Ordner wie Dokumente, Bilder, Desktop, Musik usw. an. Standardmäßig darf nur diejenige Person darauf zugreifen, die als dieser Benutzer angemeldet ist. Der nächste Schritt besteht also darin, das Benutzerkonto zu schützen.

13.1.2 Kennwörter

Kennwörter sind der wichtigste Schlüssel zum Schutz Ihrer Benutzerkonten. Nennen Sie Ihre Kennwörter niemals am Telefon. Wenn jemand Ihren Benutzernamen und Ihr Kennwort kennt, kann derjenige sich am System anmelden. Selbst wenn das Benutzerkonto nur eingeschränkte Berechtigungen besitzt (z.B. dass nur Lesen, nicht aber Bearbeiten erlaubt ist), entsteht dadurch dennoch eine Sicherheitslücke.

Achten Sie darauf, dass Ihre Benutzer vernünftige Kennwörter verwenden. Ich habe einmal ein Seminar zum Thema Sicherheit besucht, und die Referentin ließ alle Zuhörer aufstehen. Sie stellte uns dann Fragen zu unseren Kennwörtern – wenn wir eine Frage bejahten, mussten wir uns setzen. Sie begann mit Fragen wie etwa: »Verwenden Sie den Namen Ihrer Frau/Ihres Mannes als Kennwort?« oder »Verwenden Sie den Namen Ihres Haustiers?«. Nach etwa 15 Fragen standen nur noch 6 von etwa 300 Leuten! Tatsächlich wählen die meisten von uns Kennwörter, die erstaunlich leicht zu knacken sind. Verwenden Sie sichere Kennwörter: mindestens acht Zeichen lang, mit Buchstaben, Zahlen und Interpunktionszeichen.

Die Verwendung anderer als alphanumerischer Zeichen macht es aus zwei Gründen sehr viel schwieriger, ein Kennwort zu knacken. Erstens müssen Hacker bei der Verwendung nichtalphanumerischer Zeichen sehr viel mehr Zeichen als nur Buchstaben und Ziffern berücksichtigen. Zweitens verwenden die meisten Kennwort-Hacker beim Versuch, ein Kennwort herauszufinden, Kombinationen aus gebräuchlichen Wörtern und Zahlen.

Weil nichtalphanumerische Zeichen in normalen Wörtern oder Zahlen nicht vorkommen, verhindert die Verwendung beispielsweise eines Ausrufezeichens diese Hacker-Suche nach gängigen Wörtern. Allerdings erlauben nicht alle Systeme Zeichen wie @, $, % oder \. Sie müssen also ein bisschen experimentieren.

Die CompTIA empfiehlt außerdem, dass die Benutzer ihre Kennwörter regelmäßig wechseln. Das lässt sich durch eine Sicherheitsrichtlinie mit ablaufenden Kennwörtern durchsetzen, die Benutzer dazu zwingt, regelmäßig ein neues Kennwort anzugeben. Dieses Konzept hört sich theoretisch sehr gut an, ist aber praktisch kaum umsetzbar. Insbesondere vergessen Anwender ihre Kennwörter allzu leicht, wenn sich diese häufig ändern. Das kann zu noch größeren Sicherheitsproblemen führen, weil die Benutzer dann anfangen, sich ihre Kennwörter zu notieren!

Wenn in Ihrem Unternehmen häufige Kennwortwechsel vorgesehen sind, können Sie sich das Kennwort mithilfe eines Zahlensystems merken. Ich habe bei einem Unternehmen gearbeitet, in dem ich an jedem Monatsbeginn mein Kennwort wechseln musste. Das habe ich mir einfach gemacht. Ich habe ein Hauptkennwort gewählt, etwa »m3y3rs5« und dann jeweils eine Zahl angefügt, die für den Monat stand. Im Juni war es also »m3y3rs56«. Das hat tadellos funktioniert.

Hinweis

Alle Organisationen, die Wert auf Sicherheit legen, erstellen verschiedene Sicherheitsrichtlinien und sorgen für Maßnahmen, die diese gewährleisten sollen. Windows unterstützt verschiedene Mechanismen zu deren Umsetzung, wie z.B. den Zwang zur Verwendung sicherer Kennwörter. Kapitel 27 (*Computersicherheit*) befasst sich ausführlich mit der Einrichtung von lokalen Richtlinien und Gruppenrichtlinien.

Sie können in Windows darüber hinaus einen Kennworthinweis hinterlegen, der angezeigt wird, sobald Ihre Anmeldung fehlschlägt (Abbildung 13.2).

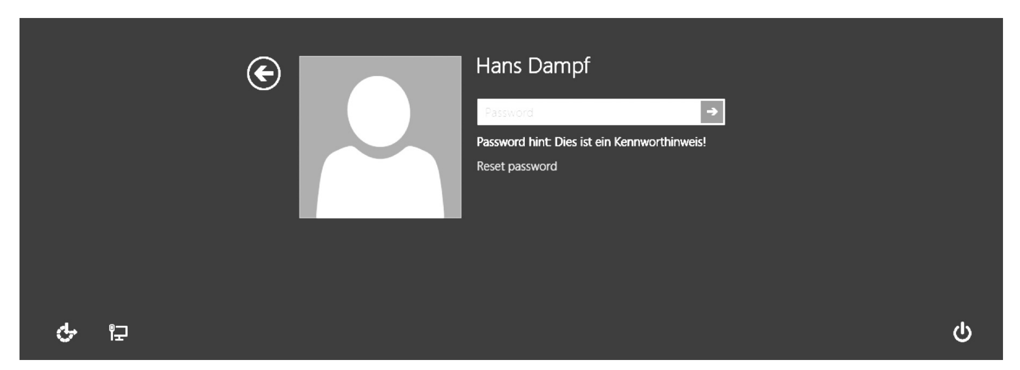


Abb. 13.2: Kennworthinweis auf dem Anmeldebildschirm

Vorsicht

Leere Kennwörter oder solche, die gut sichtbar auf Notizzetteln hinterlegt sind, bieten *keine Sicherheit*. Bestehen Sie grundsätzlich auf nicht leeren Kennwörtern und darauf, dass Kennwörter nicht offen und für jedermann sichtbar herumliegen.

13.1.3 Gruppen

Eine *Gruppe* ist einfach eine Zusammenfassung von Konten mit denselben Zugriffsberechtigungen. Ein einzelnes Konto kann Mitglied mehrerer Gruppen sein. Gruppen sind bei der Verwaltung mehrerer Benutzer unverzichtbar, insbesondere wenn man es mit vernetzten Rechnern zu tun hat. Eigenständige Computer verwenden ebenfalls Gruppen, auch wenn Windows das ein wenig verschleiert, insbesondere bei Heimanwendern.

Gruppen machen die Windows-Administration in zweierlei Hinsicht viel einfacher. Zunächst lassen sich nun einer Gruppe bestimmte Zugriffsberechtigungen für eine Datei oder einen Ordner zuordnen und müssen nicht jeweils den einzelnen Konten zugewiesen werden. Sie können eine Gruppe unter dem Namen *Buchhaltung* anlegen und für alle Beschäftigten der Buchhaltung Konten in dieser Gruppe einrichten. Wenn ein Benutzer das Unternehmen verlässt, müssen Sie sich keine Gedanken über die richtigen Berechtigungen beim Anlegen des neuen Kontos für den Nachfolger machen. Sie legen einfach ein neues Konto an und fügen den neuen Beschäftigten zu einer Gruppe hinzu! Zweitens enthält Windows bereits zahlreiche vordefinierte Benutzergruppen mit voreingestellten Zugriffsrechten.

Wie Sie sich denken können, gibt es auch hier Unterschiede zwischen den verschiedenen Windows-Versionen. Diejenigen Versionen, die sich an Heimanwender richten, verhalten sich hier ganz anders als die professionelleren Versionen. Für die Prüfung sollten Sie die folgenden Gruppen kennen:

- **Administratoren**: Alle Konten, die dieser Gruppe angehören, besitzen volle Administratorrechte. Sehr häufig gehört das Konto des Hauptbenutzers eines Windows-Systems zur Administratoren-

Gruppe. Wenn Sie also für Susi ein Benutzerkonto anlegen und sie zu einer Administratorin machen, fügen Sie der Administratoren-Gruppe ihr Benutzerkonto hinzu. Und da Administratoren auf dem System alles erlaubt ist, ist ihr ebenfalls alles erlaubt.

- **Hauptbenutzer**: Die Berechtigungen der Hauptbenutzer-Gruppe entsprechen fast denen der Administratoren-Gruppe. Allerdings können sie keine neuen Geräte installieren oder auf Dateien anderer Anwender zugreifen, sofern ihnen diese Berechtigungen für die entsprechenden Dateien oder Ordner nicht ausdrücklich eingeräumt worden sind.
- **Benutzer**: Konten der Benutzer-Gruppe können weder die Registry bearbeiten noch auf kritische Systemdateien zugreifen. Sie können zwar Benutzergruppen anlegen, dürfen aber nur die selbst angelegten Gruppen verwalten. Wenn Sie Susis Kontotyp von Administrator auf Benutzer ändern, wird ihr Benutzerkonto aus der Administrator-Gruppe entfernt und der Gruppe Benutzer hinzugefügt. Ihre persönlichen Dateien und Ordner sind davon nicht betroffen, aber was ihr auf dem System nun erlaubt ist, hat sich drastisch geändert.
- **Gäste**: Wenn jemand, der auf einem System kein Konto besitzt, sich bei diesem anmelden möchte, kann er sich dazu des Gastkontos bedienen, sofern es nicht deaktiviert worden ist. Sie könnten dieses Konto z.B. bei einer Party verwenden, um einem Gast den Zugriff auf das Internet zu ermöglichen, oder in einer öffentlichen Bibliothek. In den meisten Fällen bleibt das Gastkonto jedoch deaktiviert.

Wichtig

Beachten Sie, dass das Standardadministratorkonto *Administrator* ist. Sie sollten dieses Konto nur verwenden, wenn sich keine anderen Administratoren anmelden können. Am besten erstellen Sie ein komplexes Administratorkennwort und hinterlegen es für den Notfall in einem Safe. Ändern Sie das Kennwort des Standardadministratorkontos, um zu berücksichtigen, dass andere Benutzer der Gruppe ADMINISTRATOREN hinzugefügt wurden.

13.1.4 Standardbenutzer und erhöhte Rechte

Typischerweise gibt es auf einem Windows-Rechner ein einziges Benutzerkonto – einen Standardbenutzer – und ein lokales Administratorkonto, um wichtige Aufgaben zu erledigen, wie das Installieren oder Deinstallieren von Apps, die Aktualisierung von Software und so weiter. Wenn Sie als Standardbenutzer angemeldet sind und eine Aufgabe erledigen möchten, die ein Administratorenkonto erfordert, stehen Ihnen mehrere Möglichkeiten zur Verfügung. Sie können sich abmelden und erneut als Administrator anmelden, aber das ist ziemlich umständlich. Windows bietet die Möglichkeit, ein Hilfsprogramm per Rechtsklick und Auswahl des Kontextmenüpunkts *Als Administrator ausführen* zu starten, das dann mit *erhöhten Rechten* geöffnet wird. Wenn Sie etwas erledigen möchten, das die Berechtigungen Ihres Benutzerkontos überschreitet, tritt die *Benutzerkontensteuerung* in Erscheinung. Mehr dazu in Abschnitt 13.4, *Weitere Schutzmaßnahmen.*

13.1.5 Grundlegende Benutzerverwaltung

Zur Konfiguration lokaler Benutzerkonten und lokaler Gruppen werden Werkzeuge benötigt, mit denen sich Benutzer und Gruppen verwalten lassen. Daher gibt es in allen Windows-Versionen mindestens zwei Tools zur Benutzerverwaltung. Wir konzentrieren uns auf die einfachste Variante LOKALE BENUTZER UND GRUPPEN (Abbildung 13.3). Sie können folgendermaßen darauf zugreifen:

- Öffnen Sie in der Systemsteuerung VERWALTUNG|COMPUTERVERWALTUNG|LOKALE BENUTZER UND GRUPPEN.
- Geben Sie in das Suchfeld in der Taskleiste `lusrmgr.msc` ein und drücken Sie ↵.

Aus Gründen, die ich gleich beschreibe, gibt es in der Home-Edition von Windows 10 keine lokalen Benutzer und Gruppen.

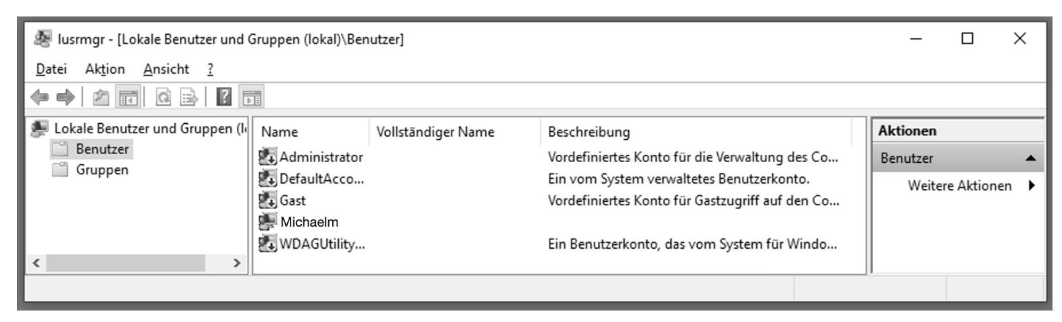


Abb. 13.3: Lokale Benutzer und Gruppen in Windows 10

Hier gibt es zwei Ordner: BENUTZER und GRUPPEN. Klicken Sie auf den Ordner BENUTZER, falls er nicht schon ausgewählt sein sollte. Sie sehen die vorhandenen Benutzer und auch den Administrator, Michaelm und Gast (Abbildung 13.3). Beachten Sie den nach unten weisenden Pfeil beim Gastkonto (und anderen), der anzeigt, dass ein Konto deaktiviert ist.

Erstellen Sie einen neuen Benutzer, indem Sie in dem leeren Bereich unter der Liste rechtsklicken und im Kontextmenü NEUER BENUTZER ... auswählen. Anschließend fügen Sie die Informationen hinzu, um einen neuen Benutzer anzulegen (Abbildung 13.4).

Standardmäßig werden alle neuen Benutzerkonten der Gruppe BENUTZER hinzugefügt. Abbildung 13.5 zeigt die in Windows 10 vorhandenen Standardgruppen. Werden Ihnen Benutzer, Hauptbenutzer, Gast und Administrator angezeigt?

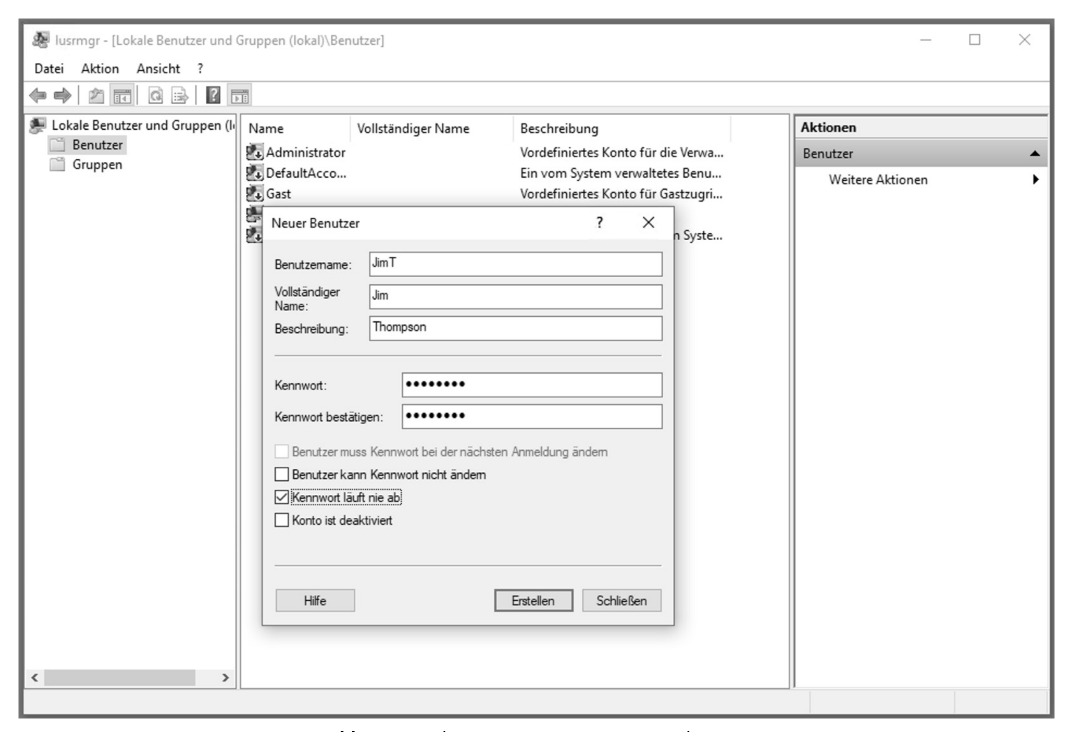


Abb. 13.4: Anlegen eines neuen Benutzerkontos

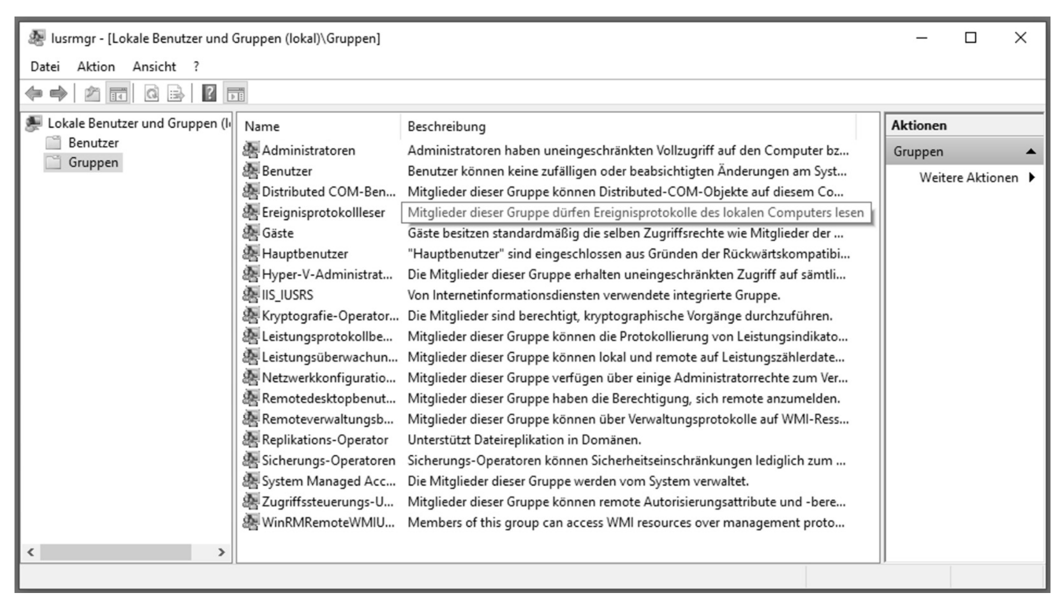


Abb. 13.5: Standardgruppen

Jetzt fügen Sie JimT zur Administratorengruppe hinzu. Doppelklicken Sie auf die Gruppe ADMINISTRATOREN und wählen Sie dann HINZUFÜGEN ... aus. Nun können Sie in das Dialogfeld BENUTZER AUSWÄHLEN `JimT` eingeben (Abbildung 13.6). Klicken Sie anschließend auf OK.

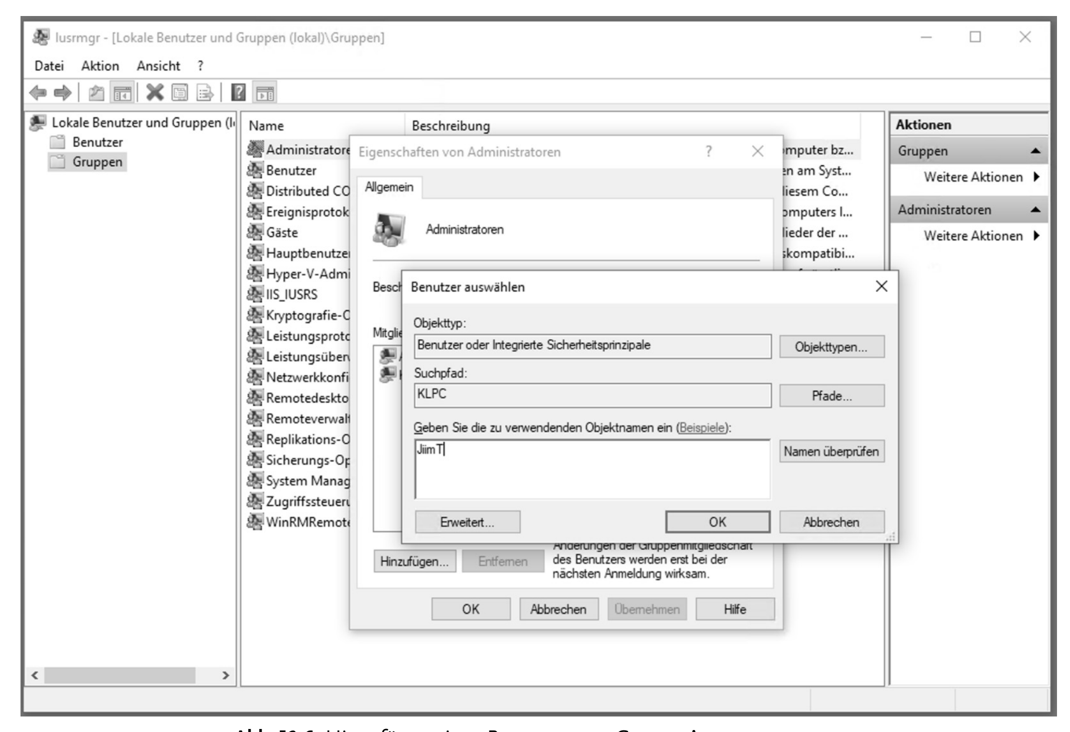


Abb. 13.6: Hinzufügen eines Benutzers zur Gruppe ADMINISTRATOREN

Sie sind natürlich nicht auf die Standardgruppen beschränkt. Wenn Sie beispielsweise eine Gruppe namens *Vormittag* anlegen möchten, wählen Sie den Ordner `Gruppen` aus, rechtsklicken in den leeren Bereich unter der Liste der vorhandenen Gruppen und wählen dann NEUE GRUPPE ... aus. Geben Sie den Namen der neuen Gruppe ein (und optional eine Beschreibung). Jetzt können Sie der Gruppe Benutzer hinzufügen (Abbildung 13.7).

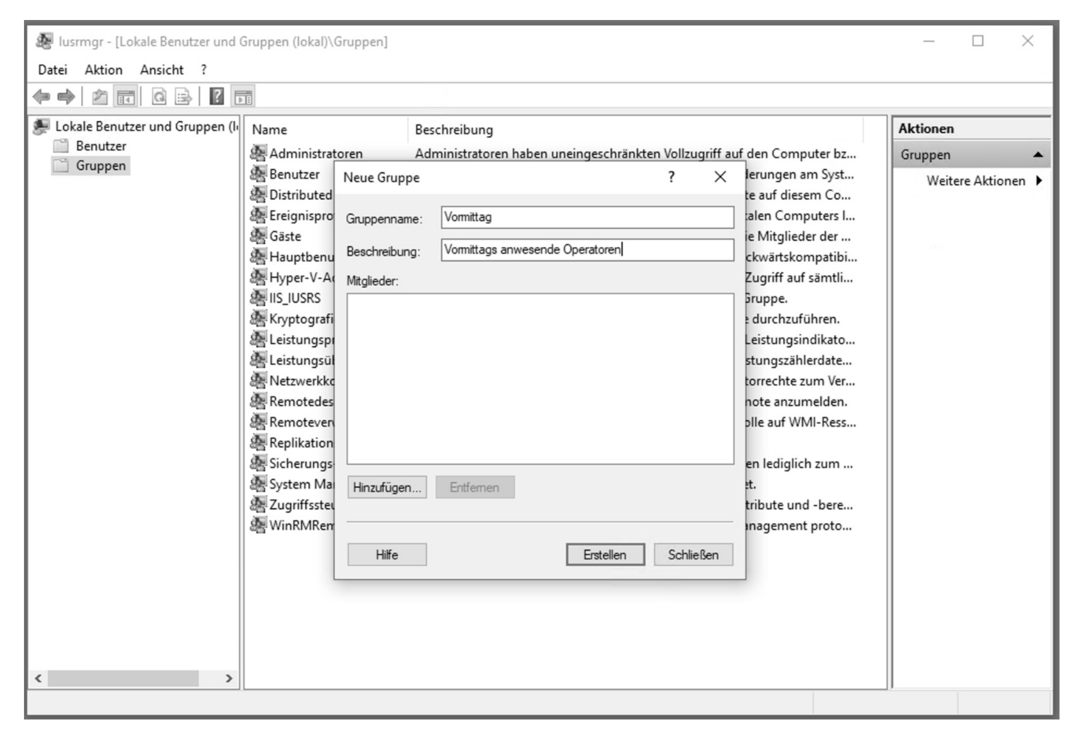


Abb. 13.7: Erstellen einer Gruppe

Hinweis

Zur Verwaltung von Benutzern müssen Sie LOKALE BENUTZER UND GRUPPEN als Administrator ausführen. Am einfachsten ist es, eine EINGABEAUFFORDERUNG (ADMINISTRATOR) zu öffnen und dort den Befehl `lusrmgr.msc` zu verwenden. In Kapitel 15, *Eingabeaufforderung*, erfahren Sie mehr über die Ausführung von Befehlen auf der Kommandozeile.

LOKALE BENUTZER UND GRUPPEN ist bestens geeignet, um die Benutzer auf einem einzelnen Windows-System zu verwalten. Microsoft bietet jedoch auch noch andere Werkzeuge an, deren Bezeichnungen sich mit den verschiedenen Versionen geändert haben. Das sehen wir uns genauer an.

Benutzerverwaltung unter Windows 7

Die Benutzerverwaltung in Windows 7 verwendet das Applet BENUTZERKONTEN, das Sie in der Systemsteuerung finden. Wenn Sie dort auf ANDERES KONTO VERWALTEN klicken, erscheint ein Fenster wie in Abbildung 13.8.

Klicken Sie nun auf NEUES KONTO ERSTELLEN, um die Optionen beim Erstellen eines neuen Benutzerkontos anzuzeigen (Abbildung 13.9). Beachten Sie, dass das Applet nur das Anlegen von Admi-

nistratorenkonten (in der Gruppe ADMINISTRATOREN) und Standardbenutzerkonten (in der Gruppe STANDARDBENUTZER) erlaubt.



Abb. 13.8: Konten verwalten

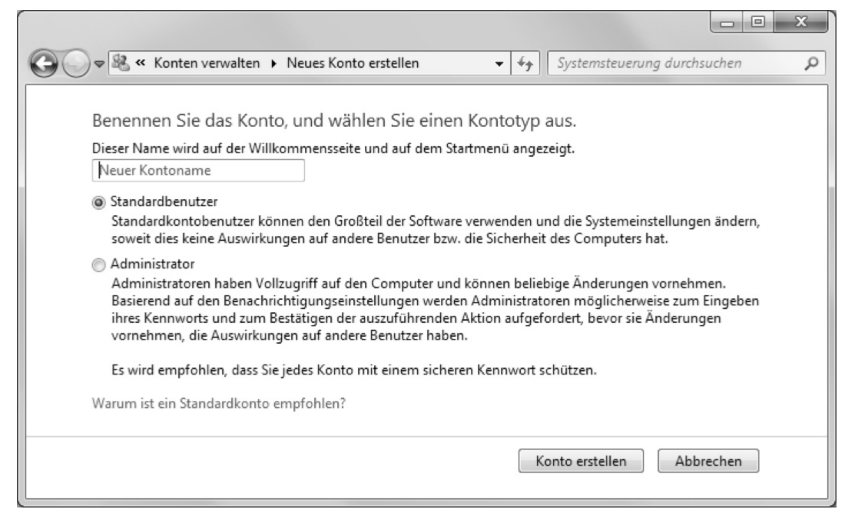


Abb. 13.9: Hinzufügen eines Benutzers

Benutzerverwaltung unter Windows 8/8.1

Seit Windows 8 konzentriert sich Microsoft weniger auf lokale Benutzerkonten als auf im gesamten Internet gültige Microsoft-Benutzerkonten. Mit Windows 8 wurde der Charm EINSTELLUNGEN einge-

führt (Abbildung 13.10).Wählen Sie dort PC-EINSTELLUNGEN ÄNDERN, um die Einstellungen zu öffnen (Abbildung 13.11) und auf die Kontooptionen zuzugreifen. Beachten Sie hier, dass Sie in der Systemsteuerung mit dem Applet BENUTZERKONTEN Änderungen an den vorhandenen lokalen Benutzerkonten vornehmen können. Sie können auch den Charm EINSTELLUNGEN aufrufen, wenn Sie ein neues Konto hinzufügen.

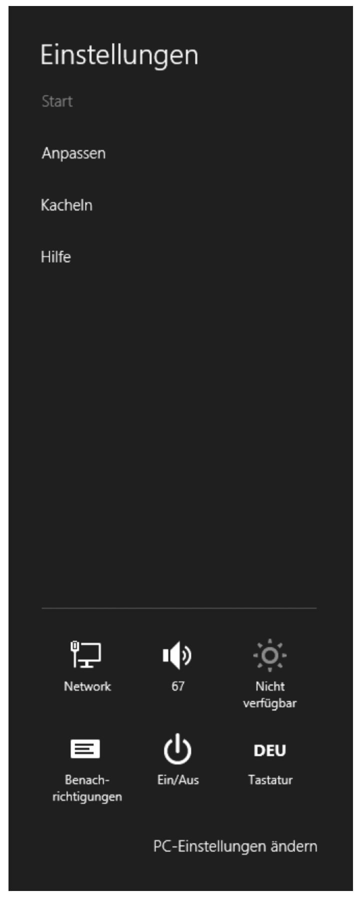


Abb. 13.10: Der Charm EINSTELLUNGEN

Wenn Sie einen PC mit Windows 8/8.1 erstmals einrichten, werden Sie ziemlich aggressiv aufgefordert, Ihr lokales Benutzerkonto aufzugeben und sich entweder mit Ihrem Microsoft-Benutzerkonto anzumelden oder solch ein Konto anzulegen. Tatsächlich macht Windows es zu einer echten Herausforderung, ein reguläres lokales Benutzerkonto alter Schule zu erstellen. Bei der entsprechenden Option wird als Beispiel eine von Microsoft gesponserte E-Mail-Adresse genannt (wie `benutzer@hotmail.com`), Sie können jedoch eine beliebige (gültige) E-Mail-Adresse für Ihr Microsoft-Benutzerkonto verwenden. Sie können stattdessen auch ein lokales Benutzerkonto erstellen, das wie ein Benutzerkonto vorheriger Windows-Versionen funktioniert. Wenn Sie sich für ein Microsoft-Benutzerkonto entscheiden, werden Ihre Fotos, Dateien und Desktop-Einstellungen (wie Hintergrundbild und Farben) synchronisiert.

Nachdem Sie ein Benutzerkonto eingerichtet haben und über ein funktionierendes System verfügen, können Sie in den PC-Einstellungen unter Konten die Anmeldeoptionen ändern, Ihr Profilbild ändern usw. Abbildung 13.12 zeigt einen typischen Bildschirm mit Kontoeinstellungen.

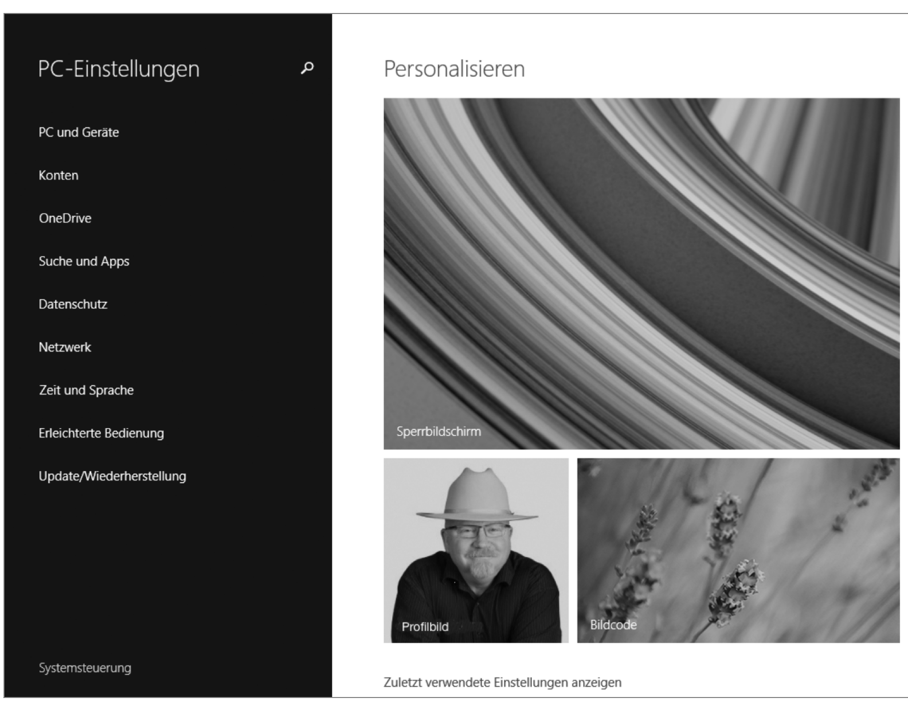


Abb. 13.11: PC-Einstellungen

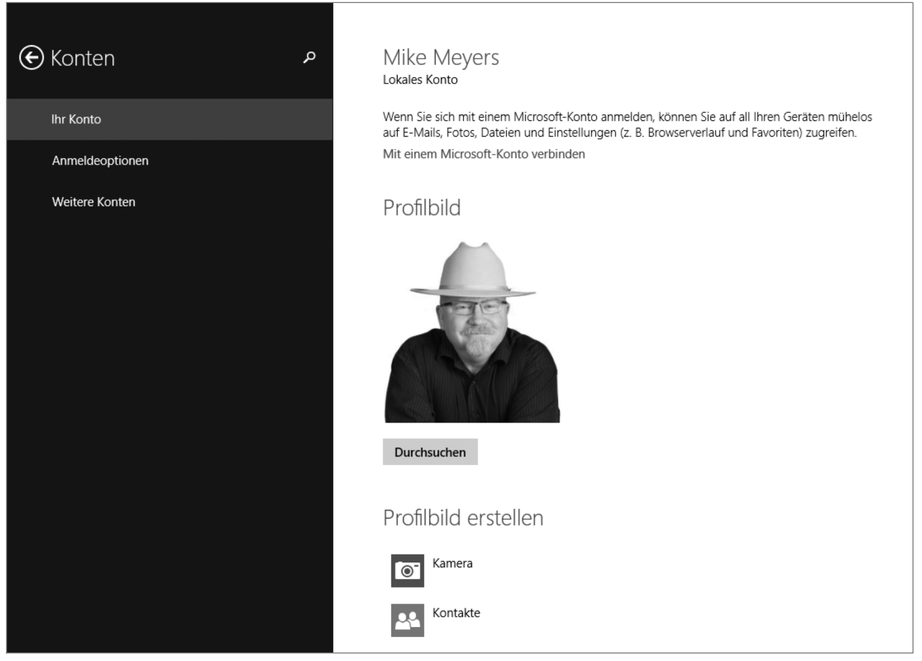


Abb. 13.12: Kontoeinstellungen in Windows 8.1

Klicken Sie auf die Option WEITERE KONTEN, um ein neues Konto zu erstellen. Nun wird der Bildschirm ANDERE KONTEN VERWALTEN angezeigt (Abbildung 13.13). Hier können Sie den Status und die Gruppenzugehörigkeit der anderen lokalen Benutzerkonten ändern. Klicken Sie auf das Pluszeichen neben dem Schriftzug KONTO HINZUFÜGEN, um loszulegen.

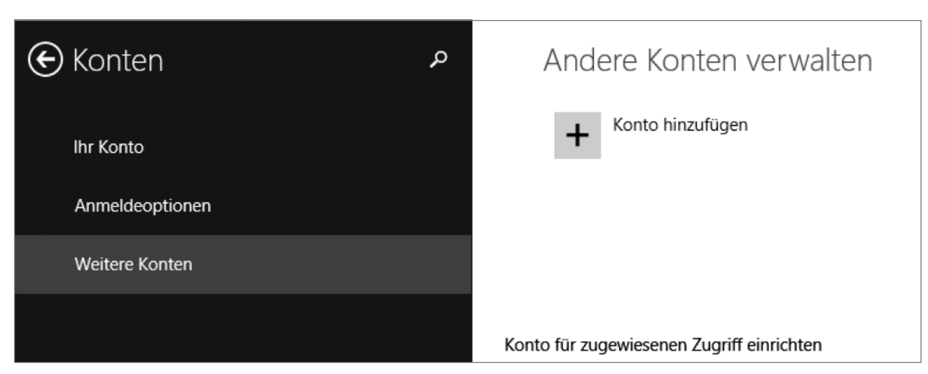


Abb. 13.13: Andere Konten verwalten

Auf dem Bildschirm WIE MELDET SICH DIESE PERSON AN? (Abbildung 13.14) gibt es die Optionen, ein vorhandenes Microsoft-Benutzerkonto anzugeben, eins einzurichten, ein Benutzerkonto für ein Kind zu erstellen oder nur ein lokales Benutzerkonto anzulegen. Die Option KONTO EINES KINDES HINZUFÜGEN erstellt ein Benutzerkonto mit aktiviertem Jugendschutz.

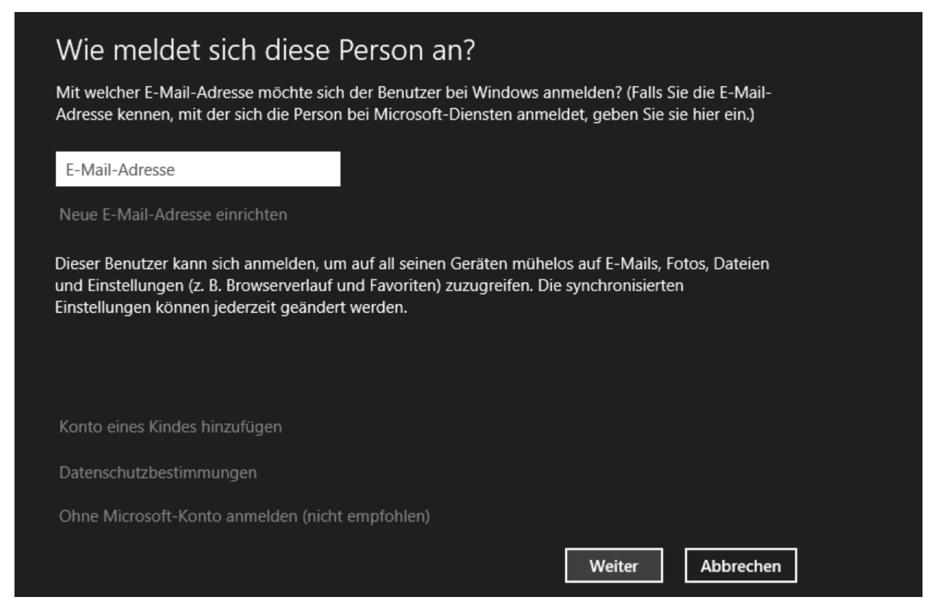


Abb. 13.14: Die Optionen beim Erstellen eines neuen Benutzerkontos

Nachdem Sie sich für ein lokales oder globales Benutzerkonto entschieden haben, erzeugt Windows dieses Benutzerkonto auf dem lokalen Rechner. Dieser Vorgang nimmt etwas Zeit in Anspruch, denn Windows erstellt die gesamte Ordnerstruktur und aktualisiert das lokale Profil des neuen Benutzers. Wenn der Vorgang schließlich beendet ist, kann sich der neue Benutzer anmelden (Abbildung 13.15).

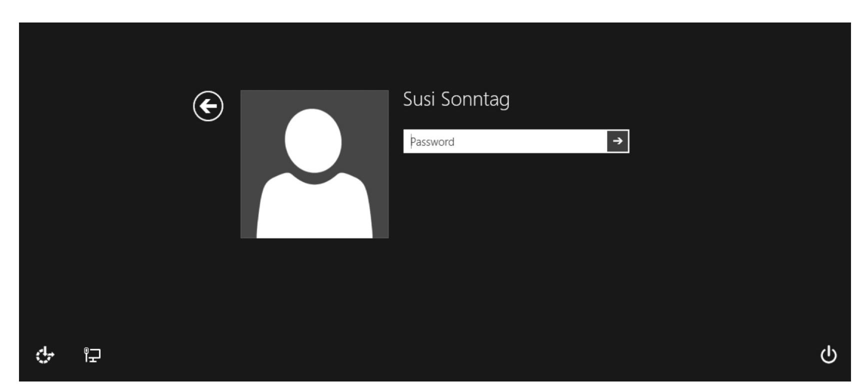


Abb. 13.15: Das neue Benutzerkonto

Benutzerverwaltung unter Windows 10

Windows 10 leidet darunter, dass Microsoft in der Vergangenheit so viele Versuche unternommen hat, eine Alternative zu LOKALE BENUTZER UND GRUPPEN zu schaffen. Deshalb gibt es drei verschiedene Werkzeuge, um Benutzerkonten und Gruppen zu verwalten. In Windows 10 wurde die App KONTEN gründlich überarbeitet und wanderte in die Einstellungen (Abbildung 13.16).

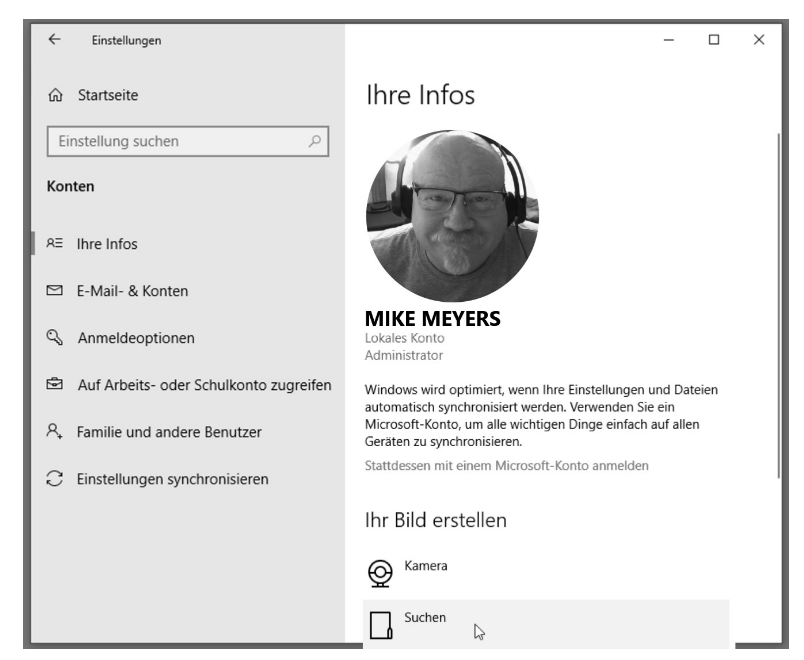


Abb. 13.16: Startseite der App KONTEN

Die App KONTEN ist eher dafür gedacht, Ihr persönliches Konto zu konfigurieren, als neue Benutzer anzulegen oder ein Benutzerkonto einer Gruppe hinzuzufügen. Sie können jedoch auch andere Benutzer bearbeiten, indem Sie FAMILIE UND ANDERE BENUTZER aufrufen und dann DIESEM PC EINE ANDERE PERSON HINZUFÜGEN auswählen (Abbildung 13.17). Aber viel Glück dabei, wenn Sie hier ein lokales Benutzerkonto anlegen möchten, denn Microsoft verbirgt diese Möglichkeit und drängt Sie dazu, ein Microsoft-Benutzerkonto zu verwenden oder anzulegen.

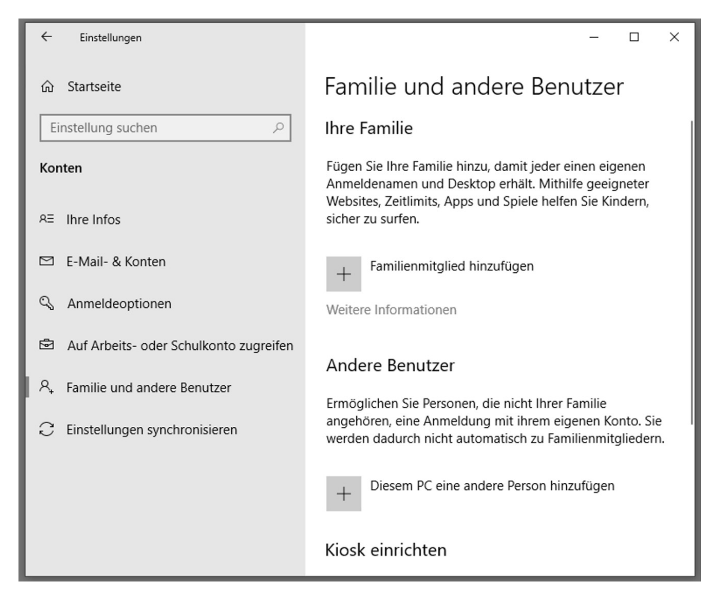


Abb. 13.17: FAMILIE UND ANDERE BENUTZER

Die App BENUTZERKONTEN in der Systemsteuerung von Windows 10 (Abbildung 13.18) ist praktisch, um Änderungen an Ihem Konto vorzunehmen, die eher technischen Charakter haben. Hier können Sie Ihre Gruppenmitgliedschaft ändern (aber nicht einrichten) und einfache Änderungen an Ihrem eigenen oder anderen Konten durchführen, wie etwa das Kennwort ändern. Sie müssen zur Gruppe der Administratoren gehören, um diese Änderungen vornehmen zu können.

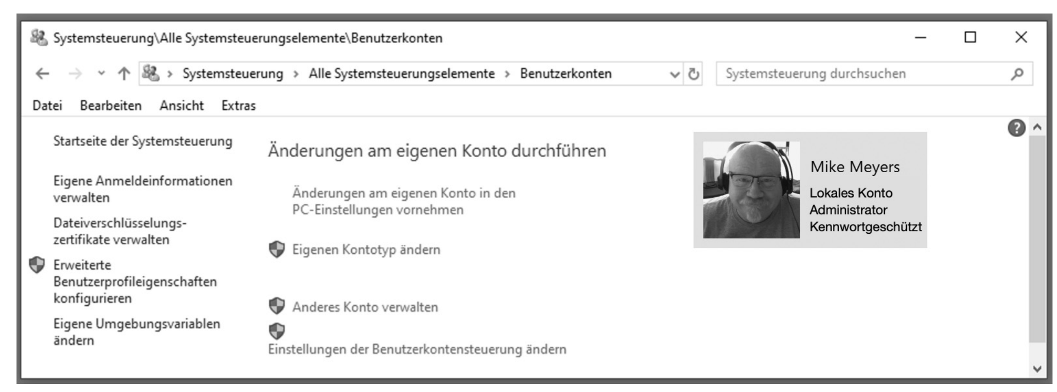


Abb. 13.18: Benutzerkonten in Windows 10

Wenn Sie nicht gerade die Home-Edition von Windows 10 verwenden, ist LOKALE BENUTZER UND GRUPPEN nach wie vor die beste Methode, wenn Sie sich darüber im Klaren sind, wie mächtig das Werkzeug ist (und nicht versuchen, etwas Gefährliches zu unternehmen, wie das Löschen des Administratorkontos).

Hinweis

Benutzer der Home-Edition von Windows 10 müssen die App KONTEN in den Einstellungen oder BENUTZERKONTEN in der Systemsteuerung verwenden.

Puh! Der ganze Trubel um lokale Benutzerkonten und Gruppen dient nur einem Zweck, nämlich einen Benutzer an einem Windows-System anzumelden. Aber sobald das erledigt ist, ist es an der Zeit, zu überprüfen, was der Benutzer mit den Daten anstellen darf. Hier kommt die Autorisierung über NTFS-Berechtigungen ins Spiel.

13.2 Autorisierung über NTFS-Berechtigungen

Benutzerkonten und Kennwörter bilden die Grundlage für den Schutz eines Windows-Rechners und ermöglichen Benutzern die Authentifizierung an einem PC. Die Autorisierung bildet die wichtige nächste Stufe bei der Sicherheit, denn sie bestimmt, wie legitime Benutzer die Ressourcen des Computers (Dateien, Ordner, Anwendungen usw.) verwenden dürfen. Windows verwendet das NT-Dateisystem und Berechtigungen zum Schutz seiner Ressourcen.

13.2.1 NTFS-Berechtigungen

Unter Windows gehört zu allen Ordnern und Dateien in einer NTFS-Partition eine Liste mit zwei Datengruppen. Erstens werden in der Liste alle Benutzer und Gruppen aufgeführt, die auf diese Ordner oder Dateien zugreifen dürfen. Zweitens gibt die Liste die Zugriffsrechte an, die für die einzelnen Benutzer oder Gruppen bei diesen Dateien oder Ordnern gelten. Die Zugriffsrechte werden über eine Reihe von Beschränkungen definiert, die *NTFS-Berechtigungen* genannt werden.

NTFS-Berechtigungen geben genau an, welche Rechte ein bestimmtes Konto hinsichtlich des Zugriffs und/oder der Bearbeitung einer Datei oder eines Ordners hat. Hier lassen sich detaillierte Angaben vornehmen, sodass dieses Werkzeug überaus mächtig ist. Beispielsweise können Sie einem Benutzer bzw. Konto zwar die Bearbeitung einer Datei erlauben, das Löschen der Datei aber unterbinden. Sie können auch einen Ordner anlegen und anderen Mitgliedern einer Gruppe die Rechte zum Anlegen von Unterverzeichnissen einräumen.

NTFS-Datei- und -Ordnerberechtigungen sind derart mächtig und kompliziert, dass komplette Bücher zu diesem Thema geschrieben worden sind! Glücklicherweise brauchen Sie für die Prüfungen zur A+-Zertifizierung nur einige Grundkonzepte der NTFS-Berechtigungen zu verstehen: Besitz, Besitzrechte übernehmen, Änderung von Berechtigungen, Ordnerberechtigungen und Dateiberechtigungen.

- **Besitz**: Wenn Sie in einer NTFS-Partition eine neue Datei oder einen neuen Ordner anlegen, werden Sie zum *Besitzer* dieser Datei bzw. dieses Ordners. Der Besitzer kann beliebige Änderungen an seinen Dateien bzw. Ordnern vornehmen und deren Berechtigungen so ändern, dass andere, selbst Administratoren, nicht darauf zugreifen können.
- **Besitzrechte übernehmen**: Alle Benutzer mit dieser speziellen Berechtigung können die Besitzrechte für Dateien/Ordner übernehmen. Administratoren-Konten haben für alles die Berechtigung »Besitzrechte übernehmen«. Beachten Sie hier den Unterschied zwischen den Besitz- und den Zugriffsrechten. Wenn Sie eine Datei besitzen, können Sie verhindern, dass andere Benutzer darauf zugreifen. Wenn Sie Administratoren die Zugriffsrechte jedoch nicht einräumen, können diese immer noch die Besitzrechte übernehmen und *anschließend* auf diese Datei zugreifen!
- **Berechtigungen ändern**: Eine weitere wichtige Berechtigung für alle NTFS-Dateien und -Ordner ist »Berechtigungen ändern«. Konten mit dieser Berechtigung können anderen Konten Berechtigungen entziehen oder gewähren.
- **Ordnerberechtigungen**: Ordnerberechtigungen legen fest, was ein Benutzer mit einem Ordner anstellen darf. Ein Beispiel hierfür ist »Ordnerinhalt anzeigen«, wodurch einem Benutzer erlaubt ist, den Inhalt eines Ordners anzuzeigen.
- **Dateiberechtigungen**: Dateiberechtigungen ähneln Ordnerberechtigungen, legen jedoch fest, was ein Benutzer mit einer bestimmten Datei anstellen darf. Ein Beispiel hierfür ist »Lesen und Ausführen«. Dem Benutzer ist in diesem Fall das Starten eines ausführbaren Programms gestattet.

Unter Windows finden Sie bei fast allen Objekten im EIGENSCHAFTEN-Dialogfeld die Registerkarte SICHERHEIT (Abbildung 13.19). Sie enthält immer zwei Hauptbereiche. Im oberen Bereich werden die

Konten mit Berechtigungen für diese Ressource aufgeführt. Im unteren Bereich wird detailliert angezeigt, welche Berechtigungen den jeweils markierten Konten eingeräumt worden sind.

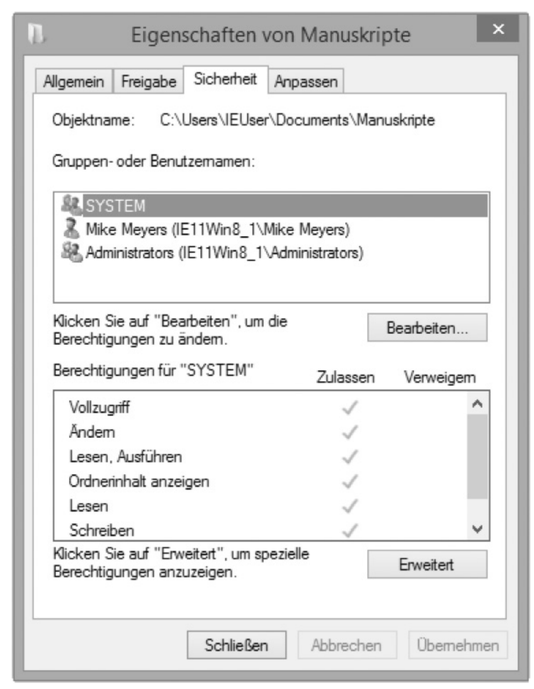


Abb. 13.19: Registerkarte SICHERHEIT

Um NTFS-Berechtigungen hinzuzufügen oder zu löschen, wählen Sie zunächst den Benutzer oder die Gruppe aus und klicken dann auf BEARBEITEN, um das Dialogfeld zum Ändern der Berechtigungen zu öffnen. Aktivieren Sie in der Spalte ZULASSEN das Kontrollkästchen neben der NTFS-Berechtigung, die Sie hinzufügen möchten. Von den Kontrollkästchen in der Spalte VERWEIGERN wird nur selten Gebrauch gemacht, denn sie erledigen eine völlig andere Aufgabe. Mehr dazu im nachfolgenden Abschnitt 13.2.2, *Vererbung*.

Die Standardberechtigungen für einen Ordner sind:

- **Vollzugriff**: Alle Aktionen lassen sich ausführen.
- **Ändern**: Lesen, Schreiben und Löschen von Dateien und Unterverzeichnissen.
- **Lesen, Ausführen**: Inhalte des Ordners und seiner Unterverzeichnisse einsehen und im Ordner enthaltene ausführbare Programme starten.
- **Ordnerinhalt anzeigen**: Inhalt des Ordners und seiner Unterverzeichnisse einsehen.
- **Lesen**: Lesen aller im Ordner enthaltenen Dateien.
- **Schreiben**: Ändern und Anlegen von neuen Dateien und Ordnern.

Dateiberechtigungen sind Ordnerberechtigungen recht ähnlich und unterscheiden sich vorwiegend hinsichtlich der Spezialberechtigungen, auf die ich weiter hinten in diesem Kapitel noch eingehen werde.

- **Vollzugriff**: Alle Aktionen sind möglich!
- **Ändern**: Lesen, Schreiben und Löschen der Datei.
- **Lesen, Ausführen**: Lesen und Ausführen der Datei (wenn es sich um ein Programm handelt).

- **Lesen**: Öffnen der Datei.
- **Schreiben**: Ermöglicht das Schreiben bzw. Speichern von Änderungen an der Datei.

Es folgen einige Regeln zum Umgang mit NTFS-Berechtigungen:

- Öffnen Sie das Dialogfeld EIGENSCHAFTEN einer Datei oder eines Ordners und wählen Sie die Registerkarte SICHERHEIT aus, um die NTFS-Berechtigungen anzuzeigen.
- NTFS-Berechtigungen werden sowohl Benutzerkonten als auch Gruppen zugewiesen. Allerdings wird es als empfehlenswert betrachtet, die Berechtigungen einer Gruppe zuzuordnen und dieser dann Benutzer hinzuzufügen, anstatt die Berechtigungen einzelnen Benutzern direkt zuzuweisen.
- Berechtigungen sind kumulativ. Wenn Sie Vollzugriff auf einen Ordner besitzen, aber lediglich über Leserechte für eine Datei in diesem Ordner verfügen, haben Sie dennoch Vollzugriff auf die Datei.
- Derjenige, der einen Ordner oder eine Datei anlegt, ist Besitzer des Objekts und verfügt über Vollzugriff.
- Falls ein Administrator auf einen Ordner oder eine Datei zugreifen möchte, benötigt er die entsprechenden Berechtigungen (die er sich durch Übernahme der Besitzrechte beschaffen kann).

Denken Sie einen Moment über diese Berechtigungen nach. Warum wurden sie von Microsoft geschaffen? Denken Sie an Situationen, in denen Sie einer Gruppe die Berechtigung »Ändern« geben würden. Sie können auch mehr als eine Berechtigung zuweisen. In vielen Situationen ist es angebracht, dass Benutzer sowohl die Berechtigung zum Lesen als auch zum Schreiben von Ordnern und Dateien haben.

13.2.2 Vererbung

Durch die *Vererbung* wird festgelegt, welche NTFS-Berechtigungen Dateien bzw. Unterordner erhalten, die in einem bestehenden Ordner neu erstellt werden. Techniker sollten wissen, wie die Vererbung funktioniert (Abbildung 13.20).

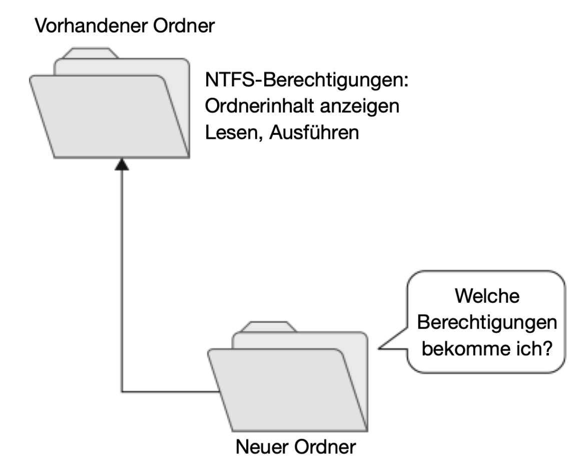


Abb. 13.20: Welche NTFS-Berechtigungen?

Grundsätzlich gilt bei der Vererbung die Regel, dass Dateien oder Ordner, die in einem anderen Verzeichnis neu erstellt werden, die NTFS-Berechtigungen dieses übergeordneten Verzeichnisses erhalten. Wenn Sie also beispielsweise für einen Ordner Lese- und Ausführberechtigung besitzen und irgendjemand eine Datei in diesen Ordner erzeugt, verfügen Sie automatisch über die Berechtigung zum Lesen und Ausführen dieser Datei (Abbildung 13.21).

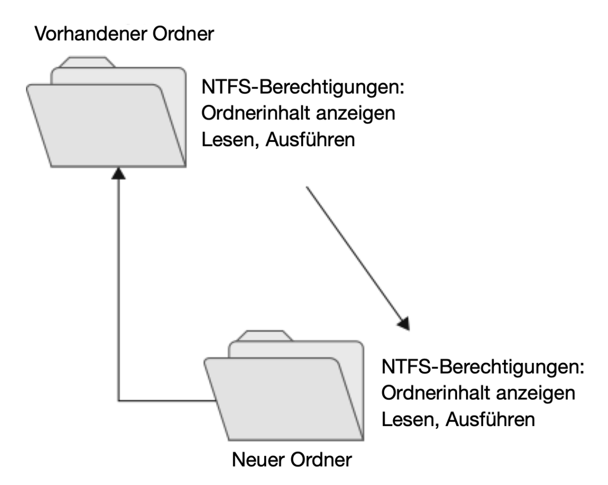


Abb. 13.21: Hier sind die Berechtigungen!

Die Vererbung ist bei allen Windows-Versionen standardmäßig aktiviert, und das ist im Allgemeinen auch gut so. Wenn Sie die EIGENSCHAFTEN eines Ordners öffnen, die Registerkarte SICHERHEIT auswählen und auf ERWEITERT klicken, wird ein Kontrollkästchen VERERBBARE BERECHTIGUNGEN DES ÜBERGEORDNETEN OBJEKTES EINSCHLIESSEN angezeigt. Hiermit könnten Sie die Vererbung deaktivieren, aber lassen Sie das lieber. Vererbung ist vernünftig und das, was man erwartet.

Wenn Sie sich Abbildung 13.22 genau ansehen, werden Sie feststellen, dass die Kontrollkästchen in der Spalte ZULASSEN bei einigen der NTFS-Berechtigungen deaktiviert sind. Auf diese Weise teilt Windows Ihnen mit, dass die fraglichen NTFS-Berechtigungen geerbt wurden. Die deaktivierten Kontrollkästchen können Sie natürlich nicht verändern. Was soll man also tun, wenn hier Änderungen vorgenommen werden müssen?

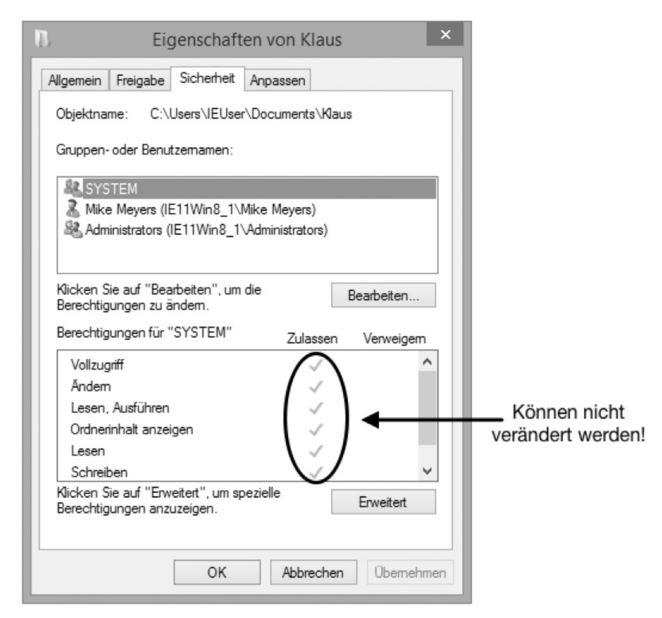


Abb. 13.22: Ererbte Berechtigungen

In seltenen Fällen kann es tatsächlich sinnvoll sein, die Vererbung für einen bestimmten Ordner oder eine einzelne Datei zu deaktivieren. Statt die Vererbung vollständig zu deaktivieren, sollten Sie besser das Kontrollkästchen in der Spalte VERWEIGERN benutzen. Das Aktivieren des VERWEIGERN-Kontrollkästchens einer NTFS-Berechtigung (Abbildung 13.23) sorgt dafür, dass Windows die Vererbung bei dieser speziellen Berechtigung ignoriert.

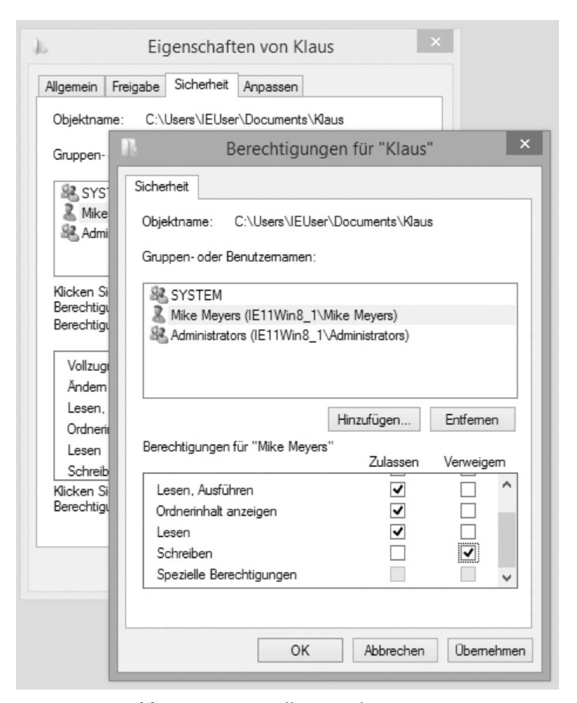


Abb. 13.23: Spezielle Berechtigungen

> **Hinweis**
>
> Das VERWEIGERN-Kontrollkästchen hat stets Vorrang vor der NTFS-Vererbung.

13.2.3 Propagieren von Berechtigungen

Beim Propagieren von Berechtigungen wird festgelegt, welche NTFS-Berechtigungen für Dateien gelten, die in einen neuen Ordner verschoben oder kopiert werden. Seien Sie hier vorsichtig! Nachdem Sie soeben die Vererbung kennengelernt haben, könnten Sie leicht auf den Gedanken kommen, dass alle Dateien und Ordner, die in einen Ordner kopiert oder verschoben werden, schlicht und einfach die NTFS-Berechtigungen dieses Ordners erben. Das ist jedoch nicht immer der Fall, und die CompTIA möchte sicherstellen, dass Sie das wissen. Tatsächlich hängen die Berechtigungen zum einen davon ab, ob die Daten kopiert oder verschoben werden, und zum anderen, ob sie vom selben Volume stammen oder nicht. Hier sind also vier Fälle zu unterscheiden:

- Daten innerhalb eines NTFS-Volumes kopieren
- Daten innerhalb eines NTFS-Volumes verschieben
- Daten von einem NTFS-Volume auf ein anderes kopieren
- Daten von einem NTFS-Volume auf ein anderes verschieben

Betrachten wir nun die Liste mit den vier Aktionen, bei denen Sie wissen müssen, was mit den kopierten oder verschobenen Objekten (Dateien oder Ordner) geschieht.

1. Wird innerhalb eines Volumes kopiert, gibt es zwei Kopien des Objekts. Die Kopie des Objekts erbt bzw. übernimmt die Berechtigungen des neuen Speicherorts. Die neue Kopie kann also andere Berechtigungen als das Original besitzen.
2. Beim Verschieben innerhalb eines Volumes gibt es nur eine Kopie des Objekts. Bei diesem bleiben die Berechtigungen unverändert erhalten.
3. Wird ein Objekt von einem NTFS-Volume auf ein anderes kopiert, entsteht eine weitere Kopie des Objekts. Die Kopie des Objekts erbt bzw. übernimmt die Berechtigungen des neuen Speicherorts. Die neue Kopie kann also andere Berechtigungen als das Original besitzen.
4. Wird ein Objekt von einem NTFS-Volume auf ein anderes verschoben, gibt es nur eine Kopie des Objekts. Das Objekt an seiner neuen Position erbt bzw. übernimmt die Berechtigungen des neuen Speicherorts. Das verschobene Objekt kann also andere Berechtigungen als das Original besitzen.

Aus der Sicht des Technikers müssen Sie einfach nur wissen, wie sich Berechtigungen beim Kopieren oder Verschieben von Dateien ändern können. Wenn Sie bei einer Datei mit sensiblen Daten Zweifel haben sollten, dann überprüfen Sie die Berechtigungen noch einmal, bevor Sie das System wieder Ihrem Kunden überlassen (Tabelle 13.1).

Vorgang	Dasselbe Volume	Anderes Volume
Verschieben	Berechtigungen bleiben erhalten.	Berechtigungen werden geerbt.
Kopieren	Berechtigungen werden geerbt.	Berechtigungen werden geerbt.

Tabelle 13.1: Berechtigungen beim Kopieren/Verschieben

Wichtig

In den aktuellen Windows-Versionen ist immer von *Volumes* die Rede, wie Sie aus Kapitel 9 wissen. Bislang wurde der Begriff *Partition* benutzt – und viele Techniker werden das auch weiterhin tun. Rechnen Sie in der Prüfung also mit beiden Begriffen.

Irgendwelche Objekte, die Sie auf einer FAT-Partition ablegen, verlieren ihre Berechtigungen, weil FAT keine NTFS-Berechtigungen unterstützt. Das gilt auch für FAT32- oder exFAT-partitionierte Massenspeichergeräte, wie die allgegenwärtigen USB-Speichersticks, die wir alle verwenden, um Dateien schnell von einem Gerät auf ein anderes zu übertragen.

13.2.4 Techniker und Berechtigungen

Um auf einem Windows-Rechner fast alles machen zu können (Updates und Anwendungen installieren, Treiber aktualisieren usw.), werden Administratorrechte benötigt. Die meisten Administratoren vergeben aber (aus offensichtlichen Gründen) nur höchst ungern Administratorberechtigungen. Wenn Ihnen jemand die Administratorrechte für einen Rechner erteilt und das System, während Sie daran arbeiten, Schaden nimmt, werden Sie sofort zum Hauptverdächtigen!

Wenn Sie an einem Windows-System arbeiten, das jemand anders administriert, sollten Sie dafür sorgen, dass derjenige Ihre Aktivitäten nachvollziehen kann und ungefähr weiß, wie lange diese voraussichtlich dauern werden. Lassen Sie sich vom Administrator ein neues Konto mit Administratorrechten anlegen. Fragen Sie nie nach dem Kennwort für ein dauerhaftes Administratorkonto! Auf diese Weise wird Ihnen nicht die Schuld zugewiesen, wenn mit dem System etwas schiefläuft: »Nun ja, als Annette die neue Festplatte installiert hat, habe ich ihr das Kennwort gegeben ... vielleicht war sie es ja!« Wenn Sie das System repariert haben, sollten Sie sich zudem davon *überzeugen, dass der Administrator das von Ihnen benutzte Konto wieder löscht.*

13.2.5 Berechtigungen in Linux und macOS

Die CompTIA A+-Zertifizierungsprüfung konzentriert sich zwar auf die Berechtigungen von Benutzern und Gruppen in Windows, an dieser Stelle darf man aber nicht vergessen, dass Linux und macOS hierfür eigene Konzepte mitbringen. Machen wir also einen kleinen Abstecher und sehen uns die Berechtigungen von Benutzern und Gruppen in Linux und macOS an. Hier sind insbesondere die Befehle `chmod` und `chown` von Interesse, da sie zu den Lernzielen der CompTIA A+-Zertifizierungsprüfung gehören.

Hinweis

Für das Verständnis dieses Abschnitts sind Kenntnisse der Kommandozeile erforderlich. Schlagen Sie gegebenenfalls in Kapitel 15, *Eingabeaufforderung*, nach, um die hier gezeigten Befehle besser nachvollziehen zu können.

Ebenso wie in Windows besitzen alle Dateien und Ordner in Linux und macOS Berechtigungen. Das ist leicht erkennbar, wenn Sie auf der Kommandozeile in Linux den Befehl `ls -l` eingeben. Er zeigt eine ausführliche Liste der Dateien und Ordner im aktuellen Arbeitsverzeichnis an. Der `ls`-Befehl wird in Kapitel 15 ausführlich erläutert, aber fürs Erste ist das ausreichend:

```
drwxrwxr-x 2 mikemeyers mi6   4096 Oct 2 18:35 agent_bios
-rw-rw-r-- 1 mikemeyers mi6  34405 Oct 2 18:39 datafile
-rwxrwxrwx 1 mikemeyers mi6   7624 Oct 2 18:39 honeypot
-rw-rw-r-- 1 mikemeyers users  299 Oct 2 18:36 launch_codes
-rw-rw-r-- 1 mikemeyers mi6    905 Oct 2 18:36 passwords.txt
```

Sehen wir uns eine Zeile dieser Ausgabe genauer an:

```
-rwxrwxrwx 1 mikemeyers mi6   7624 Oct 2 18:39 honeypot
```

Das meiste ist unwichtig: Die 1 gibt die Anzahl der Links an, `mikemeyers` ist der Besitzer und `mi6` die Gruppe. `7624` ist die Dateigröße, dann folgen Datum und Uhrzeit. Der Dateiname lautet `honeypot`.

Schenken Sie nun der Zeichenfolge `-rwxrwxrwx` Beachtung – die einzelnen Buchstaben repräsentieren die für dieses Objekt gültigen Berechtigungen. Das Minuszeichen am Anfang spielt hier keine Rolle. Es zeigt an, ob es sich bei dem Objekt um eine Datei, ein Verzeichnis oder einen Link handelt. Es verbleiben also drei Buchstabengruppen, die jeweils aus den Zeichen `rwx` bestehen. Die drei Gruppen stehen der Reihenfolge nach für

- Owner (Besitzer), die Berechtigungen des Besitzers der Datei oder des Ordners.
- Group (Gruppe), die Berechtigungen der Gruppenmitglieder der Datei bzw. des Ordners.
- Everyone (alle anderen), die Berechtigungen aller anderen.

Die Buchstaben `r`, `w` und `x` stehen für folgende Berechtigungen:

- `r` (read) Lesen des Inhalts einer Datei
- `w` (write) Schreiben oder Ändern einer Datei oder eines Ordners
- `x` (execute) Ausführen einer (Programm-)Datei oder Anzeige des Inhalts eines Ordners

Abbildung 13.24 veranschaulicht diese Beziehungen.

rwx|rwx|rwx
Besitzer
Gruppe
Alle anderen

Abb. 13.24: Berechtigungen unter Linux

Sehen wir uns ein weiteres Beispiel an:

```
-rw-rw-r-- 1 mikemeyers users 299 Oct 2 18:36 launch_codes
```

- Die Datei heißt `launch_codes`, der Besitzer bin ich und sie gehört zur Gruppe `users`.
- Der Benutzer `mikemeyers` besitzt Schreib- und Leseberechtigung (`rw-`).
- Die Gruppe `users` besitzt ebenfalls Schreib- und Leseberechtigung (`rw-`).
- Alle anderen dürfen die Datei `launch_codes` lesen (`r--`). Das sollten wir besser ändern.

Der Befehl chown

Mit dem Befehl `chown` können der Besitzer und die Gruppe einer Datei oder eines Ordners geändert werden. Für ihn gilt die folgende Syntax:

```
chown <Neuer Besitzer> Dateiname
```

Zum Ändern der Gruppe verwendet man diese Syntax:

```
chown <Besitzer>:<Gruppe> Dateiname
```

Um den Besitzer der Datei `launch_codes` auf `sally` zu ändern, geben Sie also

```
chown sally launch_codes
```

ein, und um die Gruppe auf `mi6` zu ändern:

```
chown sally:mi6 launch_codes
```

Wenn Sie nun den Befehl `ls -l` eingeben, erhalten Sie folgende Ausgabe:

```
-rw-rw-r-- 1 sally mi6     299 Oct  2 18:36 launch_codes
```

Beachten Sie, dass der Befehl `chown` Superuser-Rechte erfordert (`sudo` oder `su`), wenn Sie nicht Besitzer der Datei sind. Details dazu finden Sie in Kapitel 15.

Der Befehl chmod

Der Befehl `chmod` dient dazu, die Berechtigungen zu ändern. Leider verwendet er ein nicht gerade intuitives Nummerierungssystem:

```
r: 4
w: 2
x: 1
```

Die Berechtigungen für

```
-rw-rw-r-- 1   mi6     299 Oct  2 18:36 launch_codes
```

lassen sich folgendermaßen interpretieren:

- Die Berechtigung des Besitzers ist 6: 4+2 (`rw-`).
- Die Berechtigung der Gruppe ist ebenfalls 6: 4+2 (`rw-`).
- Die Berechtigung aller anderen ist 4: 4 (`r--`).

Der Befehl `chmod` verwendet die folgende Syntax, um Änderungen an den Berechtigungen vorzunehmen:

```
chmod <Berechtigungen> <Dateiname>
```

Dank dieser Nomenklatur können mit nur drei Zahlen alle möglichen Berechtigungen zugewiesen werden. Die aktuellen Berechtigungen lauten 664. Um die Datei vor unerwünschten Einblicken zu schützen, setzen Sie die 4 einfach auf 0 und geben den folgenden Befehl ein:

```
chmod 660 launch_codes
```

Um allen Benutzern Vollzugriff zu gewähren, erhält jeder r + w + x, also 4 + 2 + 1 = 7, und Sie verwenden folgenden Befehl:

```
chmod 777 launch_codes
```

Hinweis

Die *gebräuchlichste* Syntax für den `chmod`-Befehl verwendet drei Ziffern (zwischen 0 und 7), der Befehl kann jedoch auch vier Ziffern verarbeiten (und auch eine völlig anders aufgebaute symbolische Syntax). Geben Sie `man chmod` ein, um die Details nachzulesen.

13.3 Ressourcen sicher gemeinsam nutzen

Windows verwendet NTFS, um die persönlichen Ordner und Dateien (Dokumente, Musik, Bilder usw.) der verschiedenen Benutzer zu schützen. Anders ausgedrückt: Nur derjenige Benutzer, der diese Dokumente angelegt hat, darf auf sie zugreifen. Mitglieder der Administratoren-Gruppe können dieses Verhalten ändern, andere Benutzer (Standardbenutzer) jedoch nicht. Auf einem gemeinsam genutzten Windows-PC müssen Sie selbst aktiv werden und Ressourcen gezielt freigeben, um sie anderen Benutzern zugänglich zu machen.

Stellen Sie sich folgende Situation vor: Familie Schneider besitzt einen Computer, der als Medienserver dient, auf dem für alle Familienmitglieder Benutzerkonten eingerichtet sind. Die Schneiders könnten nun so schlau sein und ein Programm wie iTunes nutzen, mit dem es sehr einfach ist, Musik zu teilen. Sie bleiben aber beim Windows Medien Player und daher sollen alle Benutzer auf die Sammlung von MP3-Dateien zugreifen können.

Windows 7 erleichtert es durch die öffentlichen Bibliotheken für Dokumente, Musik, Bilder und Videos sehr, Daten gemeinsam zu nutzen. Öffnen Sie einfach den Explorer und klicken Sie auf das Dreieck zum Aufklappen neben einem der Bibliotheksordner, wie z.B. Musik oder öffentliche Musik. Auf die in öffentlichen Ordnern gespeicherten Daten können alle Benutzer zugreifen (Abbildung 13.25).

Windows 8/8.1/10 bieten die gleichen Bibliotheken wie Windows 7, sie werden jedoch standardmäßig nicht angezeigt. Klicken Sie mit der rechten Maustaste auf einen freien Bereich in der linken Spalte des Explorers und wählen Sie BIBLIOTHEKEN ANZEIGEN aus (Abbildung 13.26).



Abb. 13.25: Freigegebene Objekte im Ordner ÖFFENTLICH

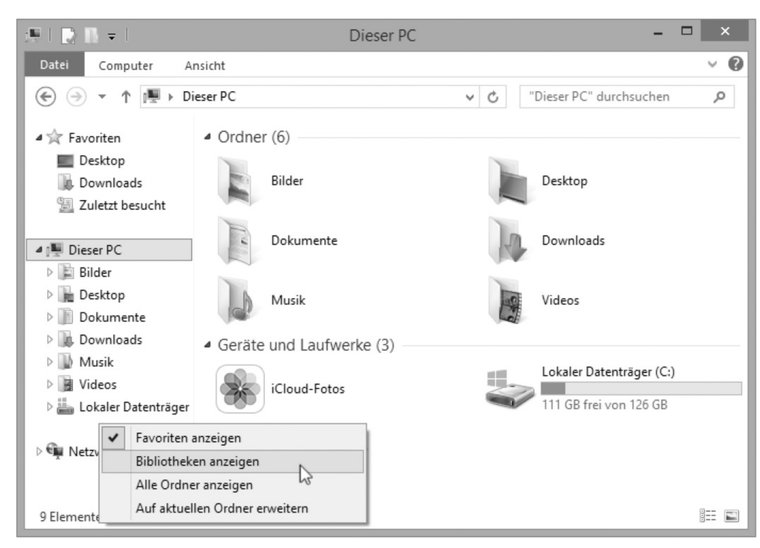


Abb. 13.26: Anzeige der Bibliotheken im Explorer von Windows 8.1

Hinweis

Wenn ein Rechner mit einem Netzwerk verbunden ist, wird die gemeinsame Nutzung von Daten viel interessanter (und komplizierter). In Kapitel 18 werden wir uns ausführlich mit diesem Thema befassen.

Nun stellt sich natürlich die Frage: Wie kann man einen Ordner, der keine Bibliothek ist, anderen Benutzern zur Verfügung stellen? Damit befasst sich der nächste Abschnitt.

13.3.1 Ordner und Dateien freigeben

Zur Freigabe von Ressourcen auf einem einzelnen Computer ist es am einfachsten, Benutzern oder Gruppen NTFS-Berechtigungen für bestimmte Ordner und Dateien zu gewähren. Klicken Sie den fraglichen Ordner oder die Datei mit der rechten Maustaste an, wählen Sie EIGENSCHAFTEN und begeben Sie sich zur Registerkarte SICHERHEIT. Die Registerkarte ist in zwei Bereiche unterteilt. Oben befindet sich eine Liste der Benutzer und Gruppen, die aktuell NTFS-Berechtigungen für das Objekt besitzen. Im unteren Bereich gibt es eine Liste der NTFS-Berechtigungen für die markierten Benutzer oder Gruppen (Abbildung 13.27).

Klicken Sie auf BEARBEITEN, um einen Benutzer oder eine Gruppe hinzuzufügen. In dem Dialogfeld BERECHTIGUNGEN, das sich nun öffnet, können Sie nicht nur neue Benutzer und Gruppen hinzufügen, sondern diese auch entfernen oder vorhandene NTFS-Berechtigungen bearbeiten (Abbildung 13.28).

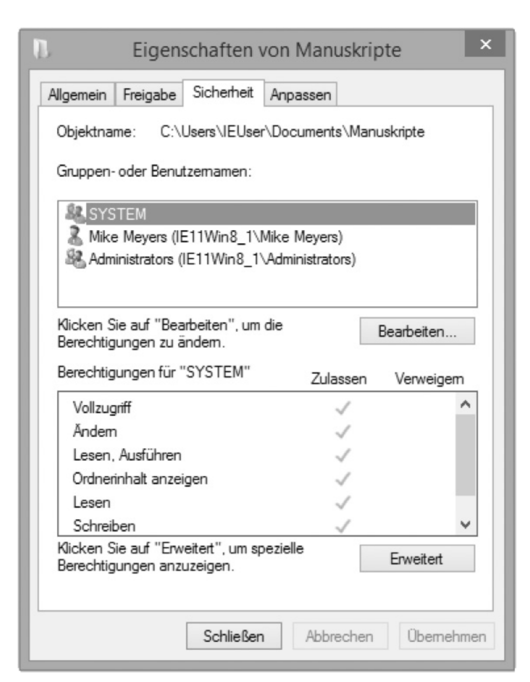


Abb. 13.27: Registerkarte SICHERHEIT

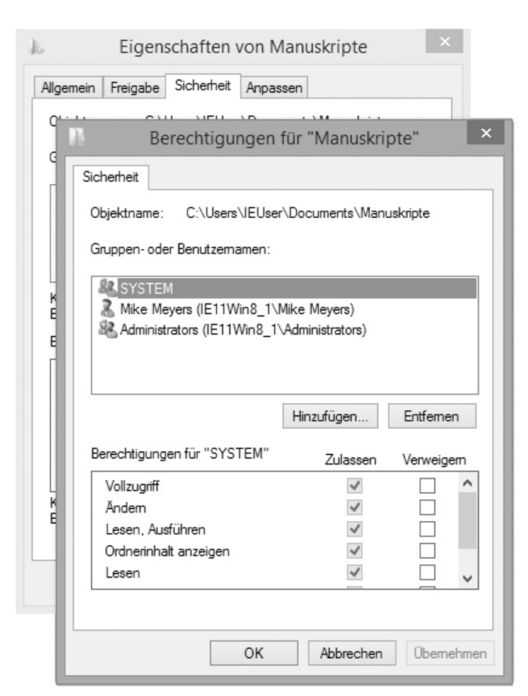


Abb. 13.28: Dialogfeld BERECHTIGUNGEN

Hinweis

Die Registerkarte FREIGABE, die in Abbildung 13.27 im Hintergrund erkennbar ist, verwendet den Freigabe-Assistenten, zu dem wir gleich noch kommen. Dabei geht es um Netzwerkfreigaben, nicht um Freigaben per NTFS.

Die soeben gezeigte Methode funktioniert zwar unter allen aktuellen Windows-Versionen, ist aber doch ein wenig altbacken. Windows stellt eine weitere Methode zur Verfügung, Daten mit anderen Benutzern zu teilen, die zwar nicht so leistungsfähig, aber einfacher anzuwenden ist. Wählen Sie irgendein Objekt aus, das Sie teilen möchten (auch eine einzelne Datei), klicken Sie es im Explorer mit der rechten Maustaste an und wählen Sie FREIGEBEN FÜR (Windows7/8/8.1) oder ZUGRIFF GEWÄHREN AUF|BESTIMMTE PERSONEN (Windows 10) aus. Nun öffnet sich das Dialogfeld Dateifreigabe (Abbildung 13.29), in dem Sie Benutzerkonten aus einem Einblendmenü auswählen können.

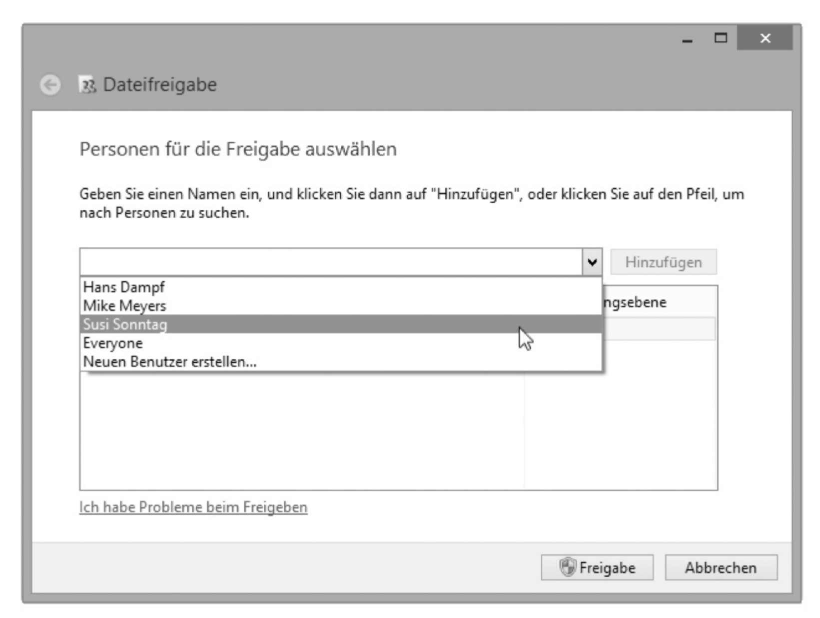


Abb. 13.29: Das Dialogfeld DATEIFREIGABE

Nachdem Sie ein Benutzerkonto ausgewählt und hinzugefügt haben, können Sie die Berechtigungsebene festlegen. Dabei stehen zwei Möglichkeiten zur Wahl: LESEN oder LESEN/SCHREIBEN (Abbildung 13.30). LESEN bedeutet, dass der Benutzer Leseberechtigung besitzt. LESEN/SCHREIBEN hingegen erlaubt dem Benutzer nicht nur das Lesen und Schreiben, sondern auch das Löschen von Dateien, die dieser Benutzer dem Ordner selbst hinzugefügt hat.

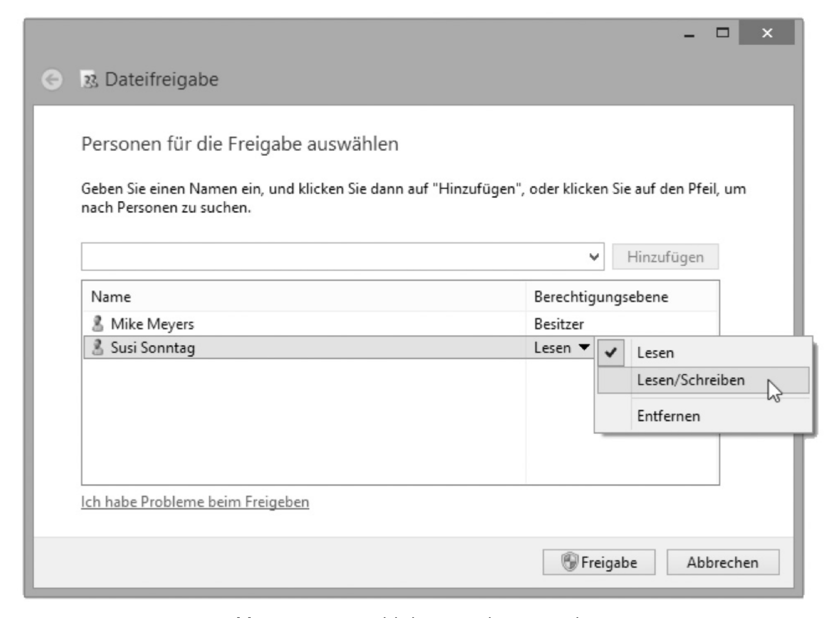


Abb. 13.30: Auswahl der Berechtigungsebene

In Windows 10 hat Microsoft dafür gesorgt, dass der Unterschied zwischen der Freigabe für andere Personen auf einem einzelnen Rechner und der Netzwerkfreigabe weniger deutlich ist. Die Freigabe erfolgt auf die gleiche Weise, aber das Dialogfeld, das nach Auswahl von ZUGRIFF GEWÄHREN AUF| BESTIMMTE PERSONEN erscheint, heißt NETZWERKZUGRIFF (Abbildung 13.31).

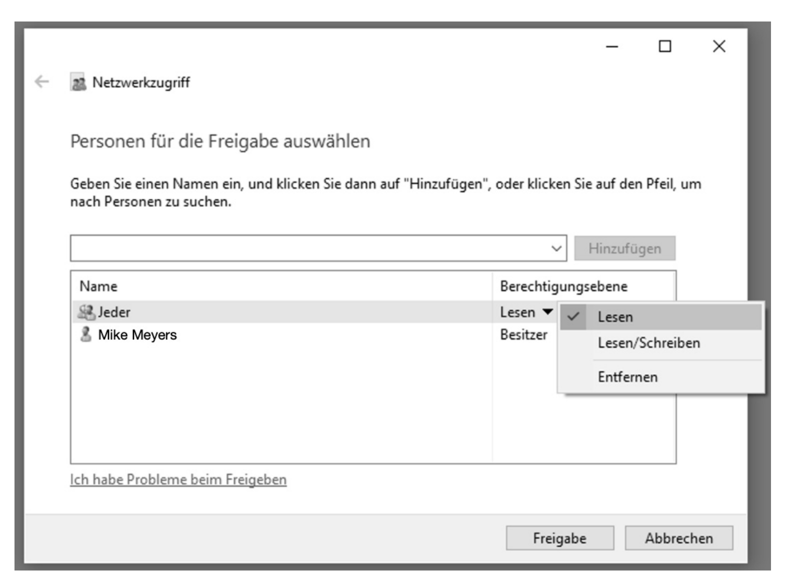


Abb. 13.31: Das Dialogfeld NETZWERKZUGRIFF in Windows 10

Hinweis

Wenn der fragliche Computer Mitglied einer Windows-Domäne ist, dann sehen die Dialogfelder DATEIFREIGABE (Windows 7/8/8.1) bzw. NETZWERKZUGRIFF (Windows 10) etwas anders aus und Sie können das Netzwerk nach Domänen-Benutzerkonten durchsuchen. Dadurch werden Freigaben im Netzwerk erleichtert. Mehr dazu in Kapitel 19.

Auffinden freigegebener Ordner

Bevor Sie sich von einem Computer entfernen, sollten Sie prüfen, ob es irgendwelche überflüssige oder (Ihnen) unbekannte freigegebene Ordner auf der Festplatte gibt. Dadurch können Sie den Computer für Benutzer besonders gut schützen. Wenn Sie den Explorer öffnen, dann springen Ihnen freigegebene Ordner insbesondere dann nicht gerade ins Auge, wenn sie sich tief im Dateisystem verbergen. Wenn das Laufwerk `C:` freigegeben ist, dann fällt das zwar sofort auf, wenn aber z.B. der Ordner `D:\temp\backup\martin\geheim` freigegeben ist, dann sieht das spätestens dann ganz anders aus, wenn keines der übergeordneten Verzeichnisse freigegeben wurde.

Windows enthält ein praktisches Hilfsmittel, mit dem sich – unabhängig vom Speicherort im Dateisystem – alle freigegebenen Ordner auf einem Rechner leicht aufspüren lassen. In der COMPUTERVERWALTUNG, die Sie über das Applet VERWALTUNG in der Systemsteuerung oder den Eintrag COMPUTERVERWALTUNG im Startmenü erreichen, gibt es unter SYSTEM die Option FREIGEGEBENE ORDNER. Darunter befinden sich drei Elemente: FREIGABEN, SITZUNGEN und GEÖFFNETE DATEIEN. Wenn Sie FREIGABEN markieren, werden Ihnen alle aktuell freigegebenen Ordner angezeigt (Abbildung 13.32).

Sie können die einzelnen Freigaben doppelklicken, um sich deren EIGENSCHAFTEN-Dialogfeld anzeigen zu lassen. Anschließend können Sie die Freigaben (z.B. Benutzer und Berechtigungen) auf die gleiche Weise wie in allen anderen Freigabe-Dialogfeldern ändern.

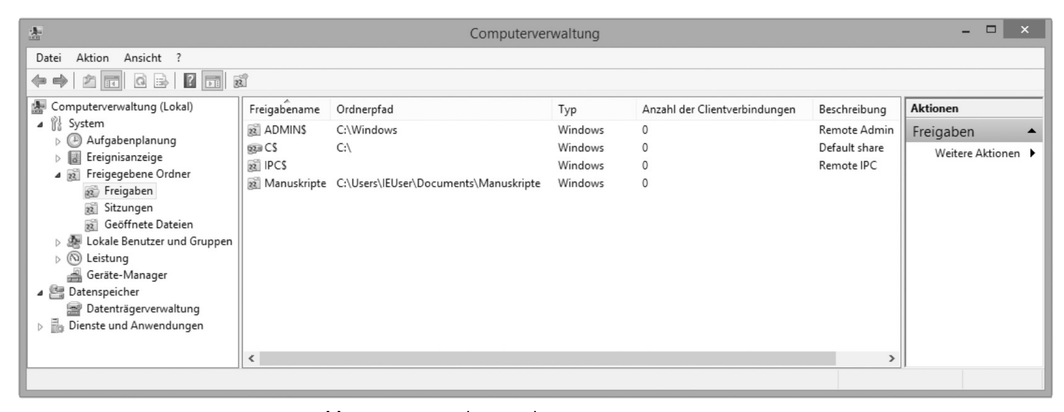


Abb. 13.32: Freigaben in der COMPUTERVERWALTUNG

13.3.2 Administrative Freigaben

Wenn Sie sich die Freigaben in Abbildung 13.32 genau ansehen, dann könnten Sie ein wenig fragend blicken und die Stirn runzeln. Was hat es denn mit Freigaben wie `ADMIN$` oder `C$` auf sich?

Bei allen Windows-Versionen seit Windows NT werden einige Standardfreigaben eingerichtet, insbesondere für alle Festplatten (nicht für optische Laufwerke, externe Festplatten oder USB-Sticks) und den Ordner `%systemroot%` (bei dem es sich üblicherweise um `C:\Windows` handelt und der als `ADMIN$` freigegeben wird). Je nach Systemkonfiguration können noch einige weitere sogenannte *administrative Freigaben* eingerichtet sein. Sie gestatten lokalen Administratoren den administrativen Zugriff auf die betreffenden Ressourcen, wenn sie sich lokal oder von einem anderen Rechner aus beim System anmelden. (Im Unterschied zu den administrativen Freigaben werden manuell eingerichtete Freigaben *lokale Freigaben* genannt.)

Administrative Freigaben sind schon ziemlich schräge Vögel. Sie können deren Berechtigungen nicht ändern. Sie können diese zwar löschen, aber dann werden sie von Windows normalerweise nach jedem Neustart wieder automatisch neu eingerichtet. Und sie bleiben verborgen, weil sie nicht angezeigt werden, wenn Sie über das Netzwerk auf den Rechner zugreifen. Sie können sie aber durchaus über deren Namen ansprechen. Wenn Sie für die Sicherheit des Administratorkennworts sorgen, gefährden diese Standardfreigaben die Gesamtsicherheit des Rechners nicht weiter.

13.3.3 Datenschutz durch Verschlüsselung

Das Codieren von Daten durch Verschlüsselungsverfahren bietet die einzige echte Möglichkeit zum Schutz Ihrer Daten vor dem Zugriff durch andere Benutzer. Administratoren können Besitzrechte übernehmen und so auf alle und auch die nicht ausdrücklich freigegebenen Dateien und Ordner auf einem Rechner zugreifen. Bei extrem geheimen Daten müssen Sie daher andere Schutzmaßnahmen implementieren. Unter den verschiedenen Windows-Versionen stehen Ihnen unterschiedlich viele Verschlüsselungsoptionen zur Verfügung. Windows Home-Editionen bringen praktisch gar keine derartigen Sicherheitsfunktionen mit. Andere Editionen bieten die *Dateiverschlüsselung* (*EFS – Encrypting File System*) und unter den professionellen Windows-Versionen kommt das Verschlüsselungssystem *BitLocker* hinzu, mit dem komplette Festplatten verschlüsselt werden können.

Dateiverschlüsselung (EFS – Encrypting File System)

Die Professional-Versionen von Windows bieten mit *EFS* (*Encrypting File System*) ein Verschlüsselungsverfahren, das alle Benutzer zur Verschlüsselung von einzelnen Dateien oder Ordnern auf einem Rechner einsetzen können.

Eine Datei oder einen Ordner zu verschlüsseln, dauert nur wenige Sekunden. Sie klicken die zu verschlüsselnden Dateien oder Ordner mit der rechten Maustaste an und wählen im Kontextmenü EIGENSCHAFTEN. In dem für das Objekt angezeigten Dialogfeld aktivieren Sie die Registerkarte ALLGEMEIN und klicken die Schaltfläche ERWEITERT an (Abbildung 13.33). Im Dialogfeld ERWEITERTE ATTRIBUTE aktivieren Sie dann das Kontrollkästchen INHALT VERSCHLÜSSELN, UM DATEN ZU SCHÜTZEN (Abbildung 13.34). Klicken Sie zweimal OK an, um erst das Dialogfeld ERWEITERTE ATTRIBUTE und dann das EIGENSCHAFTEN-Dialogfeld zu schließen. Jetzt sind Ihre Dateien oder Ordner für alle Benutzerkonten außer Ihrem eigenen verschlüsselt.

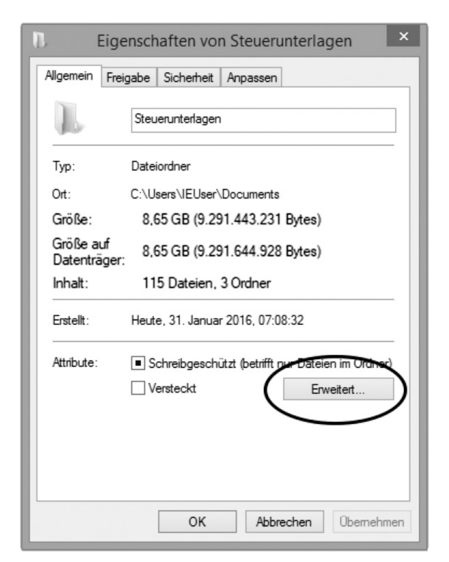


Abb. 13.33: Klicken Sie auf ERWEITERT

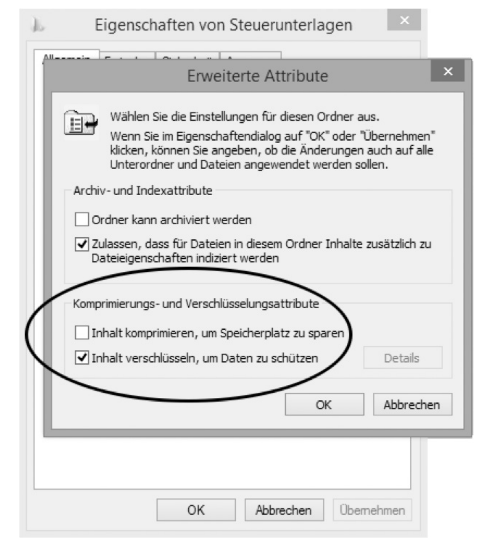


Abb. 13.34: Verschlüsselung aktivieren

Solange Ihr Kennwort geheim bleibt, sind Ihre EFS-verschlüsselten Daten vor neugierigen Augen geschützt. Diese Sicherheit hat aber ihren Preis, bei dem Ihr Kennwort eine wichtige Rolle spielt. Die Windows-Sicherheitsdatenbank speichert zwar das Kennwort (sicher und nicht im Klartext, sodass Sie darüber nicht besorgt sein müssen), aber das bedeutet auch, dass der Zugriff auf Ihre verschlüsselten Dateien von der jeweiligen Windows-Installation abhängig ist. Wenn Sie Ihr Kennwort vergessen oder wenn es von einem Administrator zurückgesetzt wird, dann kommen Sie selbst nicht mehr an Ihre verschlüsselten Daten heran. Es gibt keine Wiederherstellungsmöglichkeit. Und auch wenn der Rechner seinen Geist aufgibt und Sie durch Installation der Festplatte in einem anderen System wieder an Ihre Daten kommen wollen, haben Sie Pech gehabt. Selbst wenn Sie auf dem neuen System denselben Benutzernamen verwenden, ist die dieses Benutzerkonto definierende Sicherheitskennung anders als beim alten System. Auch dann haben Sie Pech gehabt.

Hinweis

Wenn Sie EFS nutzen, dann müssen Sie für den Katastrophenfall unbedingt einen gültigen Kennwortrücksetzdatenträger besitzen.

Dazu noch eine abschließende Warnung. Wenn Sie eine so verschlüsselte Datei auf einen Datenträger kopieren, der nicht NTFS-formatiert ist, dann wird eine Meldung angezeigt, die darauf hinweist, dass die kopierte Datei nicht verschlüsselt wird. Wenn Sie die Daten auf einen NTFS-Datenträger kopieren, bleibt die Verschlüsselung allerdings erhalten. Die verschlüsselten Dateien selbst bleiben aber, selbst wenn sie sich auf Wechselmedien befinden, nur auf dem jeweiligen System und nur für das entsprechende Benutzerkonto lesbar.

BitLocker-Laufwerkverschlüsselung

Unter Windows Ultimate und Enterprise sowie unter Windows 8/8.1/10 Pro lassen sich Laufwerke über die *BitLocker-Laufwerkverschlüsselung* vollständig verschlüsseln. BitLocker verschlüsselt das komplette Laufwerk und die Dateien aller Benutzer und arbeitet daher unabhängig von irgendwelchen Benutzerkonten. Das Schöne an BitLocker ist, dass alle Daten auf der Festplatte geschützt sind, wenn diese (nebst dem Laptop, in den sie eingebaut ist) einmal gestohlen werden sollte. Der Dieb kann darauf nicht zugreifen, selbst wenn es auf dem Laptop einen Benutzer geben sollte, der es versäumt hat, seine Daten durch EFS-Verschlüsselung zu schützen.

BitLocker funktioniert nur, wenn ein spezieller *TPM*-Chip (*Trusted Platform Module*) im Mainboard eingebaut ist. Der TPM-Chip überzeugt sich beim Start beispielsweise davon, dass es sich noch um denselben Rechner und dasselbe installierte Betriebssystem handelt und dass der Rechner nicht von irgendeinem bösartigen Programm kompromittiert wurde. Der TPM-Schutz funktioniert auch, wenn Sie das BitLocker-Laufwerk in ein anderes System einbauen.

Wenn ein gewöhnlicher BitLocker-Fehler (kein Diebstahl) auftritt, weil jemand am Laufwerk herumgebastelt hat oder das Laufwerk in ein anderes System eingebaut wurde, dann benötigen Sie einen korrekt erstellten und verfügbaren Wiederherstellungsschlüssel oder ein Wiederherstellungskennwort. Der Schlüssel oder das Kennwort wird normalerweise erstellt, wenn Sie BitLocker aktivieren, und sollte sicher verwahrt werden, z.B. als Ausdruck in einem Safe oder als Datei auf einem Netzwerkserver, auf den nur Administratoren zugreifen können.

Hinweis

Seit Windows 10 kann BitLocker einen USB-Speicherstick zum Speichern des Wiederherstellungsschlüssels verwenden, falls es keinen TPM-Chip gibt. Das ist zwar besser als nichts, aber Sie geben damit einen Teil der Sicherheit auf, die ein TPM-Chip bietet.

Um BitLocker zu aktivieren, klicken Sie in der Systemsteuerung das Symbol BitLocker-Laufwerkverschlüsselung in der klassischen Darstellung doppelt an oder wählen auf der Startseite der Systemsteuerung erst SYSTEM UND SICHERHEIT und dann BITLOCKER LAUFWERKVERSCHLÜSSELUNG. Klicken Sie dann auf BITLOCKER AKTIVIEREN (Abbildung 13.35).

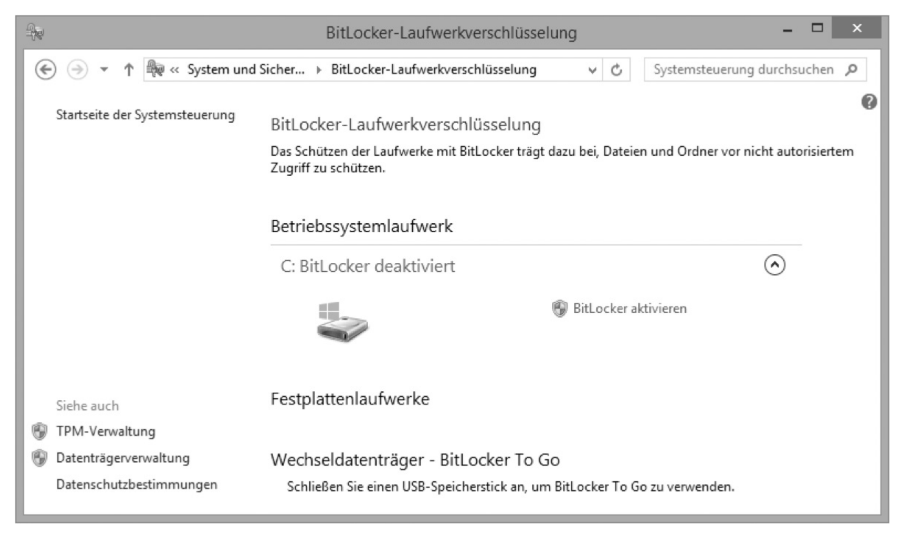


Abb. 13.35: BitLocker-Laufwerkverschlüsselung aktivieren

BitLocker To Go ermöglicht es, die Inhalte von Wechseldatenträgern wie USB-Sticks zu verschlüsseln. Der Name ist zwar fast identisch und BitLocker To Go verschlüsselt die Daten, die durch ein Kennwort geschützt sind, allerdings erfordert BitLocker To Go keinen TPM-Chip. Dennoch ist jede Maßnahme sinnvoll, wenn es darum geht, Daten zu schützen.

13.4 Weitere Schutzmaßnahmen

Wie Sie gesehen haben, sind Benutzer und Gruppen ein leistungsfähiges Werkzeug zur Authentifizierung von Benutzern und zur Autorisierung von NTFS-Berechtigungen. Das ist jedoch noch nicht alles. Es gibt zwei weitere Bereiche, in denen Benutzer und Gruppen eine Rolle spielen, die über die Anmeldung am System und die gemeinsame Nutzung von Dateien und Ordnern hinausgehen: Sicherheitsrichtlinien und Benutzerkontensteuerung. Sehen wir uns also zunächst die Sicherheitsrichtlinien an und betrachten danach die Benutzerkontensteuerung.

13.4.1 Sicherheitsrichtlinien

Sicherheitsrichtlinien sind Regeln für Benutzer und Gruppen, die so ziemlich alle möglichen Aspekte abdecken – *außer* NTFS-Berechtigungen. Möchten Sie das System so konfigurieren, dass sich die Mitarbeiter der Buchhaltung nur zwischen 9 und 17 Uhr anmelden dürfen? Dafür können Sie eine Sicherheitsrichtlinie erstellen. Und wie wäre es, wenn die Benutzer Kennwörter verwenden müssen, die mindestens acht Zeichen lang sind? Auch dafür können Sie eine Sicherheitsrichtlinie erstellen. Windows stellt Tausende voreingestellter Sicherheitsrichtlinien bereit, die Sie mit einem Werkzeug namens LOKALE SICHERHEITSRICHTLINIE aktivieren können.

Dieses Werkzeug gibt es in allen Windows-Versionen. Sie können darauf über SYSTEMSTEUERUNG|VERWALTUNG|LOKALE SICHERHEITSRICHTLINIE zugreifen, aber wir Profis öffnen die Eingabeaufforderung, geben `secpol.msc` ein und drücken ↵. Wie auch immer sie das Programm starten, es sieht ungefähr so aus wie in Abbildung 13.36.

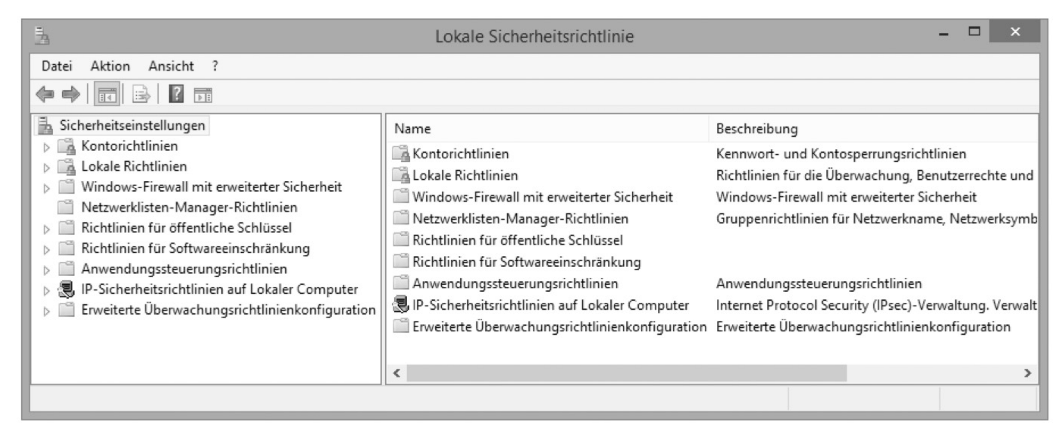


Abb. 13.36: Lokale Sicherheitsrichtlinie

> **Wichtig**
>
> Lokale Sicherheitsrichtlinien sind unglaublich leistungsfähig – tatsächlich könnte man es sich zur Lebensaufgabe machen, alles zu verstehen, was sie zu leisten imstande sind. Ich erörtere hier nur einige wenige grundlegende Fragen, die in der CompTIA A+-Zertifizierungsprüfung eine Rolle spielen können.

In der linken Spalte gibt eine Reihe von Ordnern, die dabei helfen, die vielen auf einem typischen System vorhandenen Richtlinien zu organisieren. Jeder davon enthält Unterordner oder voreingestellte Richtlinien. Als Beispiel möchte ich eine lokale Sicherheitsrichtlinie einrichten, die dafür sorgt, dass Kennwörter nach 30 Tagen ungültig werden. Für diese Richtlinie sind auch die Begriffe *Kennwortalter* oder *ablaufendes Kennwort* gebräuchlich. Öffnen Sie also den Ordner KONTORICHTLINIEN und den darin befindlichen Unterordner KENNWORTRICHTLINIEN. Sehen Sie sich den Eintrag MAXIMALES KENNWORTALTER an. In nahezu allen Windows-Versionen läuft das Kennwort eines lokalen Benutzerkontos nach 42 Tagen ab. Sie können den Wert leicht ändern, indem Sie auf MAXIMALES KENNWORTALTER doppelklicken und ihn wie in Abbildung 13.37 im Eigenschaften-Dialogfeld anpassen. Wenn Sie ihn auf 0 setzen, läuft das Kennwort niemals ab.

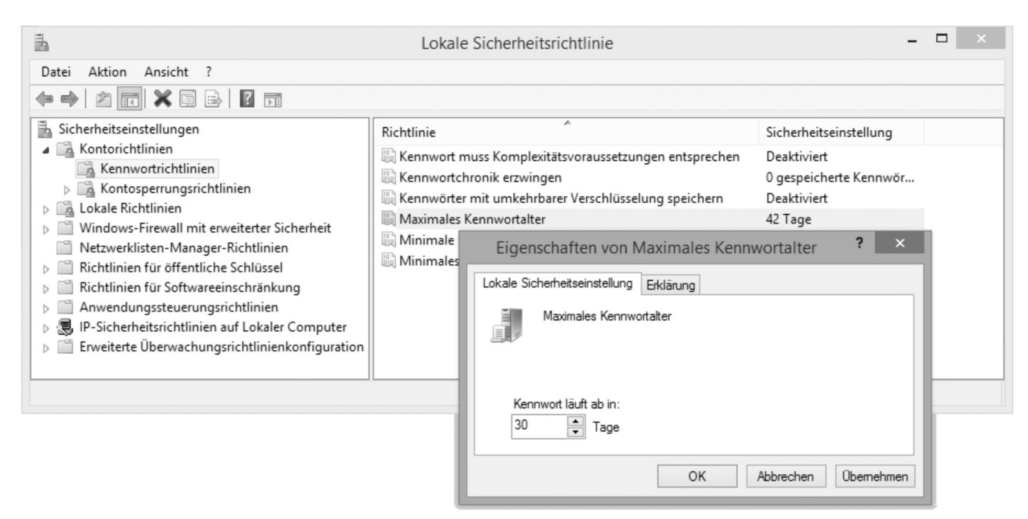


Abb. 13.37: Bearbeiten lokaler Sicherheitsrichtlinien

13.4.2 Benutzerkontensteuerung

Microsoft hat seit Windows Vista ein Feature namens *Benutzerkontensteuerung* (*UAC – User Account Control*) implementiert, das unautorisierte Änderungen an Windows verhindern soll.

Wenn man nach einem Aushängeschild für eine Liste »327 Gründe, warum wir Vista hassten« suchen würde, dürfte die Benutzerkontensteuerung in Windows Vista zu den Favoriten zählen. Die Benutzerkontensteuerung macht sich jedes Mal, wenn man versucht, *irgendetwas* auf einem System mit Windows Vista zu erledigen, als plötzlich erscheinendes Dialogfeld bemerkbar (Abbildung 13.38).



Abb. 13.38: Die Benutzerkontensteuerung in Aktion. Meine Güte!

Es ist bedauerlich, dass die Benutzerkontensteuerung einen so schlechten Ruf genießt, denn es handelt sich um eine wichtige Verbesserung der Sicherheitsfunktionen und macOS und Linux besitzen ähnliche Schutzmechanismen. Abbildung 13.39 zeigt das Äquivalent zur Benutzerkontensteuerung auf einem Mac.

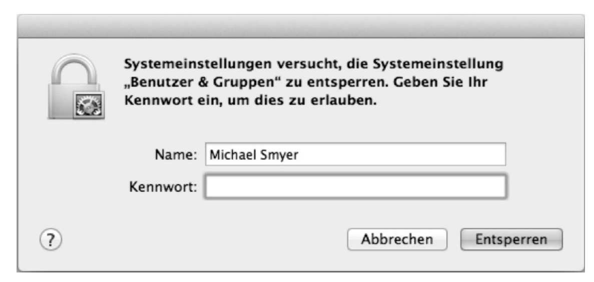


Abb. 13.39: Das Mac-Pendant zur Benutzerkontensteuerung

Warum wurde Microsoft dann so sehr für die Benutzerkontensteuerung in Windows Vista gescholten, wenn doch die anderen Betriebssysteme Ähnliches verwenden? Der Grund dafür ist einfach: Windows-Anwender sind total verzogen und die große Mehrheit hatte – bis zum Erscheinen der Benutzerkontensteuerung – keine Vorstellung davon, wie gefährlich und verantwortungslos ihr Verhalten am Computer war.

Die Probleme begannen vor Jahren, als Microsoft NTFS entwickelte. NTFS verwendet sichere Benutzerkonten und ermöglicht eine feine Steuerung der Zugriffsmöglichkeiten auf Dateien und Ordner, aber das hat seinen Preis. NTFS ist – in der ursprünglichen Form – ziemlich kompliziert.

Benutzerkonten haben schon immer eine gewisse Herausforderung bedeutet. Das Administratorkonto ist das einzige Benutzerkonto, dem wirklich alles auf einem Windows-System gestattet ist. Selbstverständlich können Sie ein System mit Gruppen einrichten, denen Sie NTFS-Berechtigungen zuweisen – das ist in größeren Netzwerken mit Vollzeitkräften in der IT Alltag. Aber was ist mit kleinen Büros und Heimnetzwerken? Diese Anwender besitzen nur äußerst selten die erforderlichen Kenntnisse, um sich mit den Schwierigkeiten bei der Einrichtung von Benutzern und Gruppen auseinanderzusetzen. Das Ergebnis sind Systeme, in denen sämtliche Benutzerkonten standardmäßig Administratorrechte besitzen. Und dann wird es riskant (Abbildung 13.40).



Abb. 13.40: Eine der drohenden Gefahren, wenn Administratorrechte in den falschen Händen liegen

Die Benutzerkontensteuerung warnt Benutzer, wenn sie im Begriff sind, Aktionen mit ernsthaften Folgen durchzuführen. Microsoft nennt für solche Aktionen, die Administratorrechte erfordern, eine Reihe von Beispielen:

- Installieren und Deinstallieren von Programmen
- Installation von Gerätetreibern (z.B. für eine Digitalkamera)
- Installation von Windows-Aktualisierungen
- Anpassung von Einstellungen der Windows-Firewall
- Ändern des Kontentyps eines Benutzers
- Durchsuchen von Verzeichnissen anderer Benutzer

Vor dem Erscheinen von Vista hatte Microsoft das Konzept einer speziellen Hauptbenutzergruppe entwickelt, deren Mitglieder über viele Berechtigungen eines Administrators verfügen (um beispielsweise viele der oben aufgeführten Aktionen durchzuführen), ohne diese Benutzer tatsächlich zu Administratoren zu machen. Natürlich muss weiterhin irgendjemand die Benutzer dieser Gruppe zuordnen, daher wurde diese Hauptbenutzergruppe von den Anwendern in kleinen Büros und Heimnetzwerken weitgehend ignoriert (Abbildung 13.41).

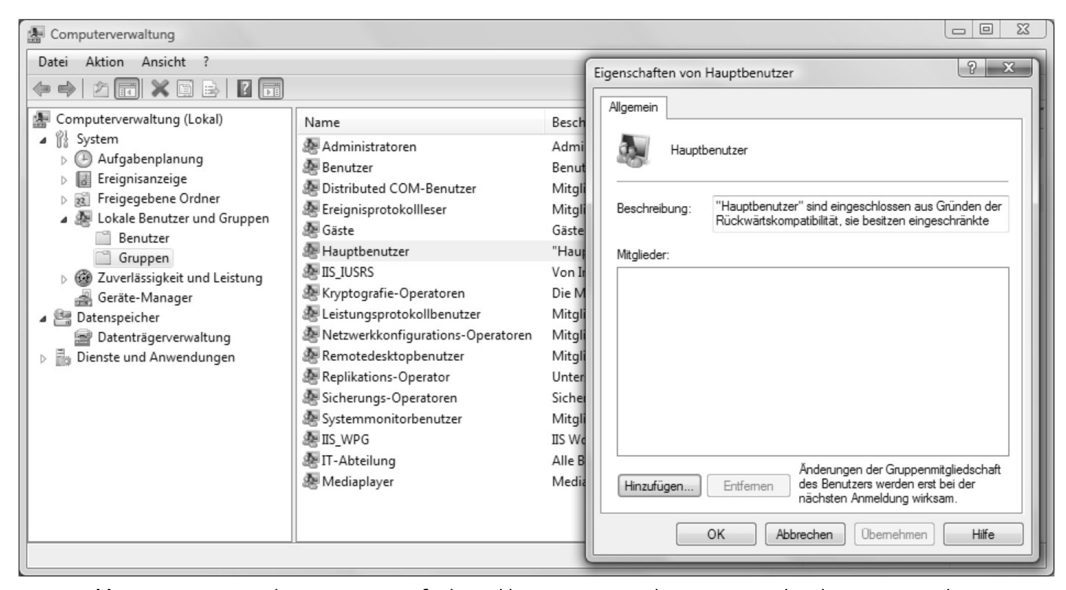


Abb. 13.41: Die Hauptbenutzergruppe findet in kleinen Büros und Heimnetzwerken kaum Verwendung.

Es war offensichtlich, dass eine bessere Methode gefunden werden musste, um die Leute davon abzuhalten, Programme auszuführen, von denen sie besser die Finger lassen sollten. Wenn ein Benutzer die entsprechenden Zugriffsberechtigungen besitzt (oder sich beschaffen kann), sollte es so einfach wie möglich sein, die erforderlichen Aufgaben durchzuführen. Dazu waren folgende Änderungen notwendig:

- Die Vorstellung, dass für die alltägliche Arbeit ein Administratorkonto erforderlich ist, muss aus den Köpfen der Menschen verschwinden.
- Alle Benutzerkonten sollen die für sie vorgesehenen Aufgaben möglichst einfach erledigen können.
- Wenn ein normaler Benutzer eine Aufgabe erledigen möchte, für die Administratorrechte erforderlich sind, muss der Benutzer ein Administratorkennwort eingeben.
- Wenn ein Benutzer mit Administratorrechten eine Aufgabe erledigen möchte, für die Administratorrechte erforderlich sind, muss der Benutzer sein Kennwort nicht erneut eingeben, aber eine »Sind Sie sicher?«-Meldung bestätigen (das berüchtigte Dialogfeld der Benutzerkontensteuerung), damit er sich der Bedeutung der Aktion bewusst ist.

Hinweis

Sowohl Linux als auch macOS nutzen schon seit geraumer Zeit eine Art Benutzerkontensteuerung auf der Kommandozeile – sie heißt `sudo`. Lesen Sie in Kapitel 15 nach.

13.4.3 Funktionsweise der Benutzerkontensteuerung

Die Benutzerkontensteuerung steuert sowohl normale Benutzerkonten als auch solche mit Administratorrechten. Wenn ein normaler Benutzer versucht, eine Aktion durchzuführen, für die Administratorrechte benötigt werden, wird das Dialogfeld der Benutzerkontensteuerung angezeigt, das zur Eingabe des Administratorkennworts auffordert (Abbildung 13.42).

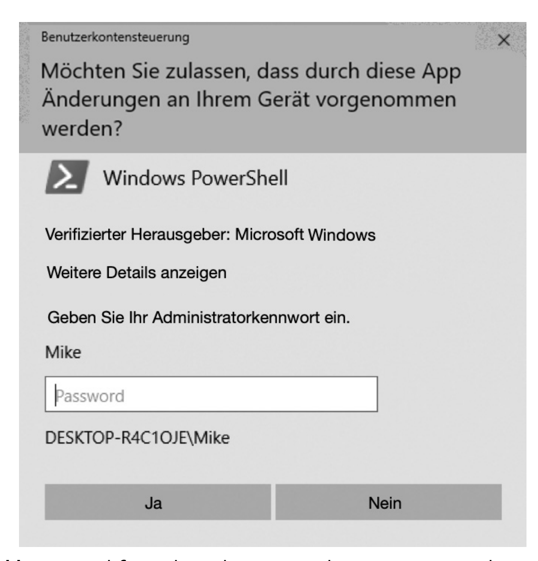


Abb. 13.42: Abfrage des Administratorkennworts in Windows 10

Falls hingegen ein Benutzer mit Administratorrechten eine solche Aufgabe erledigen möchte, erscheint eine vereinfachte Meldung (Abbildung 13.43).

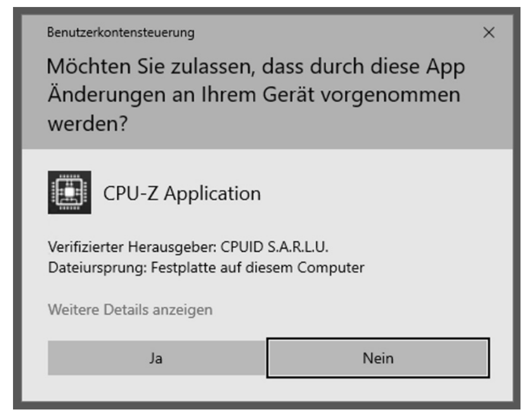


Abb. 13.43: Die Zustimmungsaufforderung

Hinweis

Die offizielle Bezeichnung des Dialogfelds in Abbildung 13.43 lautet ZUSTIMMUNGSAUFFORDERUNG.

Die Benutzerkontensteuerung verwendet kleine Schutzschild-Symbole, um Sie vorab davor zu warnen, dass Sie bei bestimmten Aktionen befragt werden (Abbildung 13.44). Wie Sie bald sehen werden, hat Microsoft diese etwas überflüssige Funktion in nachfolgenden Windows-Versionen aktualisiert.

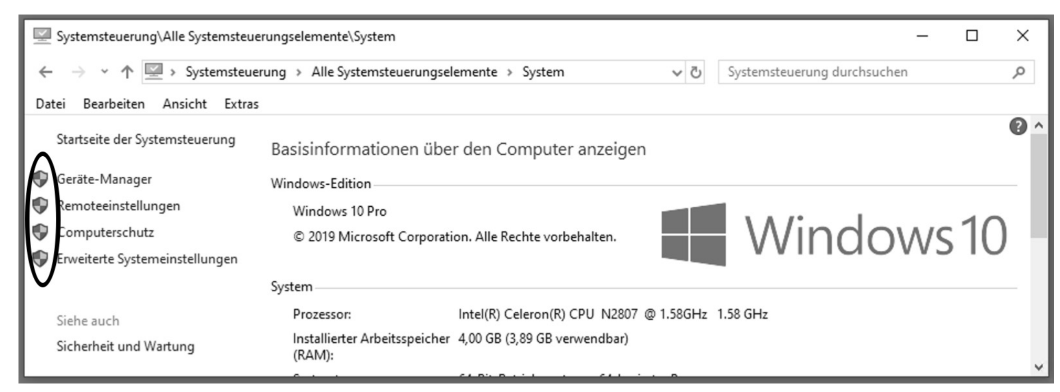


Abb. 13.44: Schutzschild-Symbole

Die Benutzerkontensteuerung gibt Benutzern beim Start eines Programms die Möglichkeit zu überdenken, was sie da gerade tun. Das ist an sich eine gute Sache, aber die verwöhnten Windows-Anwender sind es nicht gewohnt, die Folgen ihres Handelns zu berücksichtigen. Daher wollten die meisten Anwender nach dem Erscheinen von Vista wissen, wie man die Benutzerkontensteuerung abschalten kann. Das ist zwar durchaus möglich, aber es ist ganz einfach, die Auswirkungen der Benutzerkontensteuerung zu reduzieren.

13.4.4 Benutzerkontensteuerung moderner Windows-Versionen

Microsoft ist zwar ein ziemlich großes Unternehmen, nimmt aber Klagen der Benutzer über ungeliebte Funktionen dennoch ernst. Mit Windows 7 wurde daher eine verbesserte, weniger brüskierende Benutzerkontensteuerung vorgestellt, deren Verwendung deutlich vereinfacht wurde. Diese Form der Benutzerkontensteuerung findet sich auch in allen nachfolgenden Windows-Versionen.

Feiner abgestimmte Benutzerkontensteuerung

Microsoft hat untersucht, warum die Benutzerkontensteuerung die Benutzer so auf die Palme treibt, und festgestellt, dass die Benutzerkontensteuerung selbst gar nicht das Problem ist, sondern die Tatsache, dass man entweder ständig von ihr unterbrochen wird oder aber (wenn sie abgeschaltet ist) überhaupt keine Hilfestellung erhält. Um dieses aggressive Verhalten der Benutzerkontensteuerung abzumildern, führte Microsoft vier verschiedene Stufen für die Benutzerkontensteuerung ein. Geben Sie unter Windows 10 `Benutzerkontensteuerung` in das Suchfeld in der Taskleiste ein und wählen Sie unter den Treffern EINSTELLUNGEN DER BENUTZERKONTENSTEUERUNG ÄNDERN aus. Es erscheint ein Dialogfeld mit einem Schieberegler zum Einstellen dieser Stufe (Abbildung 13.45). Sie können auch das Applet BENUTZERKONTENSTEUERUNG in der Systemsteuerung öffnen und EINSTELLUNGEN DER BENUTZERKONTENSTEUERUNG ÄNDERN auswählen (Abbildung 13.46). (Diese Option gibt es in Windows 7/8/8.1/10.)

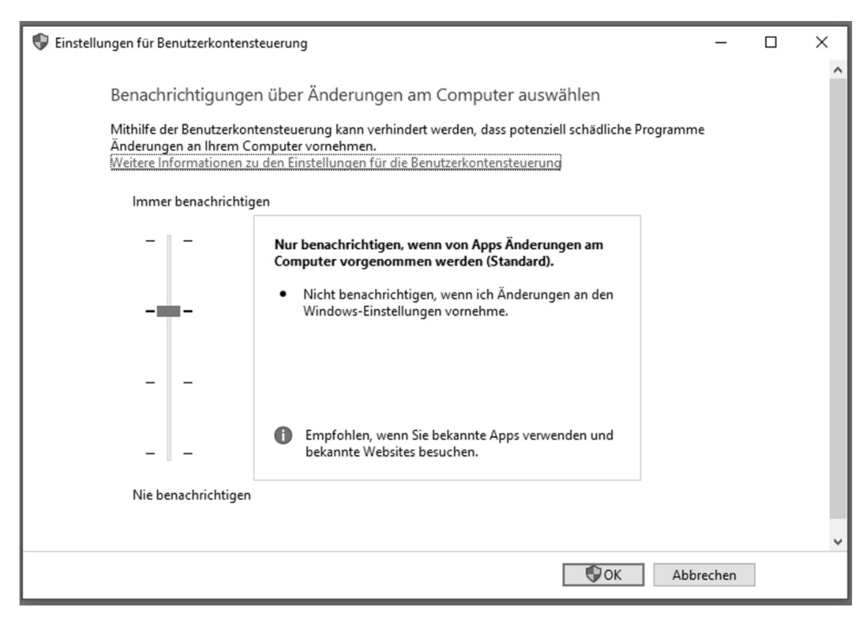


Abb. 13.45: Die vier Stufen der Benutzerkontensteuerung

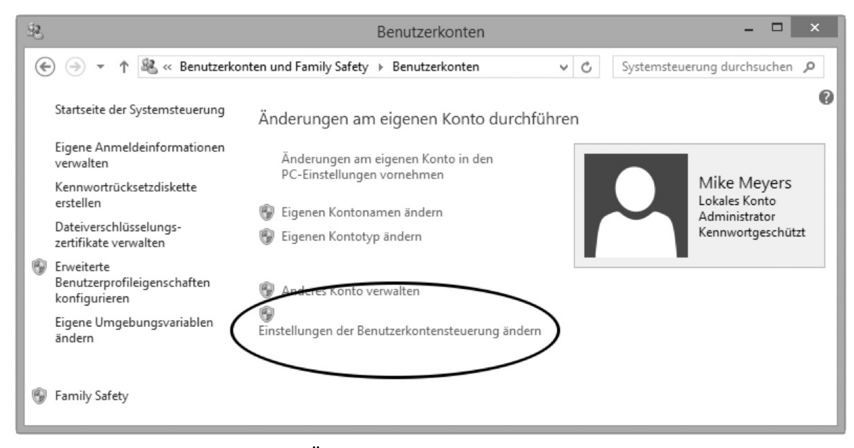


Abb. 13.46: Die Option zum Ändern der Einstellungen der Benutzerkontensteuerung

In Abbildung 13.45 ist der Schieberegler mit den vier Stufen erkennbar. Die oberste Stufe (IMMER BENACHRICHTIGEN) bedeutet, dass die Benutzerkontensteuerung genau so arbeitet wie in Windows Vista und stets ein Dialogfeld anzeigt, wenn Sie etwas erledigen möchten, für das Administratorrechte erforderlich sind. Die unterste Stufe (NIE BENACHRICHTIGEN) deaktiviert die Benutzerkontensteuerung. Die beiden mittleren Stufen sind neu und einander sehr ähnlich. Beide Stufen bewirken Folgendes:

- Beim Durchführen von Änderungen keine Benachrichtigung anzeigen.
- Benachrichtigung anzeigen, wenn ein Programm versucht, eine Änderung durchzuführen.

Der Unterschied besteht in der Art und Weise, *wie* die Benachrichtigung angezeigt wird. Die zweithöchste Stufe zeigt die bekannte Zustimmungsaufforderung an, wenn ein Programm versucht, Änderungen durchzuführen. Hierbei wird der Rest des Bildschirms abgedunkelt und Sie müssen, bevor Sie

fortfahren können, die Zustimmungsaufforderung bestätigen oder ablehnen. Bei der zweitniedrigsten Stufe wird die Benachrichtigung hingegen in Form eines gewöhnlichen Dialogfelds angezeigt.

Wichtig

Die vier Stufen der Benutzerkontensteuerung sollten Sie beherrschen.

Änderungen durch Programme und selbst durchgeführte Änderungen

Was genau ist denn der Unterschied zwischen Änderungen durch Programme und Änderungen, die ich selbst durchführe? Betrachten Sie Abbildung 13.47. In diesem Fall ist die Benutzerkontensteuerung auf die zweithöchste Stufe eingestellt. Das Installationsprogramm für den Adobe Acrobat Reader (das der Farbe der Titelleiste nach zu urteilen überprüft wurde) versucht, eine Erweiterung zu installieren. Da es sich um ein Programm handelt, das Änderungen vornehmen möchte, wird der Bildschirm abgedunkelt und die Zustimmungsaufforderung angezeigt.

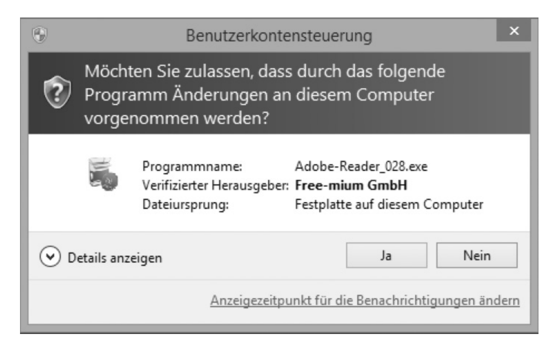


Abb. 13.47: Zustimmungsaufforderung vor abgedunkeltem Bildschirm

Wenn die Benutzerkontensteuerung auf die zweitniedrigste Stufe eingestellt ist, erscheint ebenfalls die Zustimmungsaufforderung, die sich aber wie ein normales Dialogfeld verhält.

Wichtig

Für die Benutzerkontensteuerung ist in Windows die zweithöchste Stufe voreingestellt, was zu einer Meldung wie derjenigen in Abbildung 13.47 führen würde.

Das Verhalten bei Änderungen durch ein Programm (wie das eben erwähnte von Adobe) unterscheidet sich also deutlich vom Versuch, selbst eine Änderung vorzunehmen. Beachten Sie die Schutzschildsymbole (siehe Abbildung 13.46).

Bei diesen Optionen handelt es sich nicht um Programme, sondern lediglich um in Windows eingebaute Funktionen. Durch die Schutzschildsymbole wird Ihnen signalisiert, dass zum Ändern der daneben befindlichen Funktion Administratorrechte benötigt werden. Hätten Sie die höchste Stufe der Benutzerkontensteuerung eingestellt, bekämen Sie beim Klick auf eine der Optionen eine Zustimmungsaufforderung angezeigt. Bei allen anderen Stufen können Sie die Optionen ohne Zustimmungsaufforderung verwenden. Das gilt natürlich nicht, wenn Sie keine Administratorrechte besitzen. Als Standardbenutzer werden Sie, wie in Windows Vista, zur Eingabe eines Administratorkennworts aufgefordert.

Dank der in Windows 7 vorgenommenen Verbesserungen ist die Benutzerkontensteuerung nun für jedermann geeignet. Sie mag hier und da noch für eine Überraschung oder Verärgerung sorgen, aber dieses eine »Möchten Sie zulassen, dass ...?«-Dialogfeld könnte sehr wohl den Unterschied zwischen einem sicheren und einem unsicheren Computer ausmachen.

13.5 Wiederholung

13.5.1 Fragen

1. Welches Werkzeug bzw. welcher Mechanismus legt fest, welche Ressourcen einem Benutzer zugänglich sind und was er mit ihnen anstellen darf?

   A. Authentifizierung durch Benutzerkonto und Kennwort

   B. Autorisierung durch Benutzerkonto und Kennwort

   C. Authentifizierung durch NTFS

   D. Autorisierung durch NTFS

2. Was wäre das beste Kennwort für den Benutzer Jochen, dessen Haustier Purzel heißt, und der am 8. Januar 1982 geboren ist?

   A. Jochen1982

   B. JochenliebtPurzel

   C. 1982Winter

   D. oddvr88*

3. Wie können Sie ein ganzes Laufwerk verschlüsseln, die Dateien und Ordner anderer Benutzer eingeschlossen?

   A. EFS

   B. Benutzerkontensteuerung

   C. Administrative Freigaben

   D. BitLocker

4. Welche Funktion sorgt unter Windows 7 dafür, dass für Standardbenutzer eine Zustimmungsaufforderung angezeigt wird, in der sie Anmeldedaten eines Administrators eingeben können, um verschiedene Aufgaben erledigen zu können, die ansonsten Administratoren vorbehalten bleiben?

   A. Befehl `Benutzerzugriff`

   B. Benutzerzugriffssteuerung

   C. Befehl `Benutzerkonto`

   D. Benutzerkontensteuerung

5. Mit welcher Berechtigung kann ein Administrator die Besitzrechte einer Datei ändern, ohne das Kennwort des Benutzerkontos für diese Datei zu kennen?

   A. Ändern

   B. Besitzrechte ändern

   C. Besitz

   D. Besitzrechte übernehmen

6. Sie kopieren eine Datei von einem Ordner auf einer NTFS-formatierten Festplatte, die für alle Benutzer nur lesbar ist, auf einen USB-Stick mit FAT32-Dateisystem. Welche effektiven Berechtigungen besitzt die so erstellte Kopie der Datei?

   A. Nur lesbar für alle

   B. Vollzugriff für alle

   C. Keine

   D. Dateien lassen sich von NTFS-Laufwerken nicht auf FAT32-Laufwerke kopieren.

7. Welcher der folgenden Befehle wird in Linux zum Ändern der Berechtigungen von Dateien verwendet?

   A. `chmod`

   B. `chown`

C. `users`

D. `pwn`

8. Welches Werkzeug in Windows 8.1 erlaubt es, anhand eines globalen Microsoft-Benutzerkontos ein neues Benutzerkonto zu erstellen?

   A. Benutzerkonten in der Systemsteuerung

   B. Benutzer und Gruppen in der Systemsteuerung

   C. Charm EINSTELLUNGEN

   D. Charm BENUTZER

9. Welche Funktion erlaubt es, auf einem einzelnen Windows-8-System Dateien mit anderen Benutzern zu teilen?

   A. Ablegen der Dateien in öffentlichen Bibliotheken

   B. Ablegen der Dateien in öffentlichen Freigaben

   C. Ablegen der Dateien im EFS-Ordner

   D. Das geht nicht. Windows verhindert die gemeinsame Nutzung von Dateien auf einzelnen Systemen.

10. Mit welchem der folgenden Dateisysteme können Sie Dateien so verschlüsseln, dass sie mit allen Konten außer dem eigenen nicht mehr angezeigt werden können?

   A. EFS

   B. FAT

   C. FAT32

   D. OSR

13.5.2 Antworten

1. **D.** Die Autorisierung durch NTFS legt fest, welche Ressourcen einem Benutzer zugänglich sind und was er mit ihnen anstellen darf.
2. **D.** *oddvr88** wäre von den aufgeführten Alternativen das beste Kennwort. Es enthält ein nicht alphanumerisches Zeichen, durch das es für Hacker schwerer zu knacken ist.
3. **D.** Die Laufwerkverschlüsselung mit BitLocker erlaubt es, ein ganzes Laufwerk, die Dateien und Ordner anderer Benutzer eingeschlossen, zu verschlüsseln.
4. **D.** Die Funktion *Benutzerkontensteuerung* unter Windows 7 sorgt dafür, dass Standardbenutzern eine Zustimmungsaufforderung angezeigt wird, in der sie Administrator-Anmeldedaten eingeben können, um verschiedene Aufgaben ausführen zu können, die normalerweise Mitgliedern der Gruppe ADMINISTRATOREN vorbehalten bleiben.
5. **D.** Mit der Berechtigung *Besitzrechte übernehmen* kann ein Administrator die Besitzrechte einer Datei ändern, ohne das Kennwort des Benutzerkontos für die Datei zu kennen.
6. **C.** Hier ist es wichtig, dass Sie die Datei von einer NTFS-Festplatte auf ein USB-Laufwerk mit FAT32-Dateisystem kopieren. Dabei wird eine zweite Kopie des Objekts erstellt. Die Kopie des Objekts am neuen Speicherort besitzt überhaupt keine Berechtigungen.
7. **A.** In Linux wird der Befehl `chmod` verwendet, um die Berechtigungen von Dateien zu ändern.
8. **C.** In Windows 8.1 können Sie den Charm EINSTELLUNGEN dazu verwenden, anhand eines globalen Microsoft-Benutzerkontos ein Benutzerkonto zu erstellen.
9. **A.** Mit öffentlichen Bibliotheken können Sie Dateien mit anderen Benutzern teilen.
10. **A.** Mit dem EFS-Dateisystem können Sie Dateien so verschlüsseln, dass sie nur noch über Ihr eigenes Konto angezeigt werden können.

Wartung und Optimierung 14

Themen in diesem Kapitel:

- Durchführung von Wartungsaufgaben
- Optimierung
- Vorbereitungen treffen

Alle modernen Betriebssysteme müssen gelegentlich optimiert und ständig gewartet werden, damit es nicht zu Fehlern kommt. Microsoft, Apple und die vielen Linux-Entwickler nutzen ihre jahrzehntelangen Erfahrungen im Bereich der Betriebssysteme und suchen stets nach Möglichkeiten, die Wartung und die Fehlersuche weniger beschwerlich zu gestalten und hochgradig zu automatisieren. Es gibt aber noch immer genug zu tun, um die Dinge am Laufen zu halten.

Dieses Kapitel beginnt mit der Beschreibung von Wartung und Optimierung, deshalb möchte ich hier diese Begriffe klären. Die *Wartung* beschreibt Aufgaben, die Sie regelmäßig ausführen, damit das Betriebssystem seine Leistung behält. Dazu gehören beispielsweise die Dienstprogramme für die Festplatte. CompTIA betrachtet die Optimierung als Aufgaben, die Sie ausführen, damit Ihr System eine bessere Leistung zeigt – ein gutes Beispiel dafür ist der Einbau zusätzlichen Arbeitsspeichers. Dieses Kapitel beschreibt Standardaufgaben bei der Wartung und Optimierung von Windows, macOS und Linux sowie die Werkzeuge, die Techniker dafür einsetzen.

Hinweis

In diesem Kapitel werden typische Aufgaben bei der Wartung und Optimierung aller Betriebssysteme erläutert, die derzeit zur CompTIA A+-Zertifizierungsprüfung gehören. Entsprechend des Marktanteils konzentriere ich mich dabei eher auf Windows und weniger auf macOS und Linux.

Auch ein perfekt gewarteter und optimierter Computer bekommt früher oder später Probleme. Festplatten fallen aus, leichtsinnige Kollegen löschen Dateien und die tolle neue Grafikkarte will einfach nicht funktionieren. Solche Probleme lassen sich kaum vermeiden, Sie sollten aber sicherstellen, dass Sie darauf vorbereitet sind, wenn die Schwierigkeiten auftauchen. Dieser Bereich wird von vielen Anwendern vernachlässigt und als Techniker ist es Ihre Aufgabe, die Fehlerbehebung so reibungslos wie nur möglich zu gestalten. Die Entwickler der Betriebssysteme liefern viele Werkzeuge, mit denen man sich auf Probleme vorbereiten kann, sie müssen aber auch genutzt werden.

1002

14.1 Wartung von Betriebssystemen

Betriebssysteme benötigen Patches; Massenspeichergeräte müssen richtig organisiert werden, damit sie vernünftig funktionieren. Die Registry und die temporären Dateien müssen gelegentlich aufgeräumt werden. Früher mussten viele dieser Aufgaben von Hand erledigt werden, aber heute erledigen die Betriebssysteme viele oder sogar die meisten dieser Aufgaben automatisch. In diesem Abschnitt betrachten wir die gängigsten Wartungsaufgaben, die Techniker an Systemen vornehmen. Er endet mit Erläuterungen zu benutzerdefinierten Werkzeugen für die Wartung von Windows.

14.1.1 Patchverwaltung

Es gibt kein fehlerloses Betriebssystem. Zum einen bieten alle Betriebssystemhersteller ständig verbesserte Features an, zum anderen gibt es böse Buben, die Schwachstellen entdecken und Schadsoftware entwickeln, um diese auszunutzen. Die sichere und möglichst zeitnahe Aktualisierung der Software wird als *Patchverwaltung* bezeichnet. Von dem Moment an, in dem Microsoft eine neue Windows-Version veröffentlicht, zwingen Angriffe durch Schadsoftware, Programmierfehler, neue Hardware, neue Funktionen und viele andere Dinge Microsoft dazu, Updates für das Betriebssystem bereitzustellen, die in der Computerwelt allgemein als *Patches* bezeichnet werden. Eine Patchverwaltung ist nicht nur unter Windows erforderlich, sie muss auch bei Linux und macOS erfolgen. Dazu komme ich ebenfalls.

Patchverwaltung unter Windows

Microsoft handhabt die Patchverwaltung vornehmlich durch eine Einstellung-App bzw. ein Applet der Systemsteuerung namens WINDOWS UPDATE. In seiner mehr als zwei Jahrzehnte währenden Geschichte hat Windows Update viele Änderungen erlebt. Glücklicherweise ist die CompTIA nur daran interessiert, dass Sie die Funktionsweise unter Windows 7 und neueren Systemen kennen.

Windows 7 unterscheidet bei den verfügbaren Fehlerbehebungen zwischen zwei Typen: Updates und Service Packs. Bei *Updates* für Windows 7 handelt es sich um individuelle Fehlerbehebungen, die relativ häufig (etwa wöchentlich) veröffentlicht werden. Sie sind meist eher klein und selten mehr als ein paar Megabyte groß. Ein *Service Pack* hingegen ist eine riesige Zusammenstellung von Updates und zusätzlichen Inhalten, die Microsoft hinzufügt. Service Packs sind daher unweigerlich sehr groß (mehrere Hundert Megabyte) und werden oft zusammen mit Windows vertrieben (Abbildung 14.1).

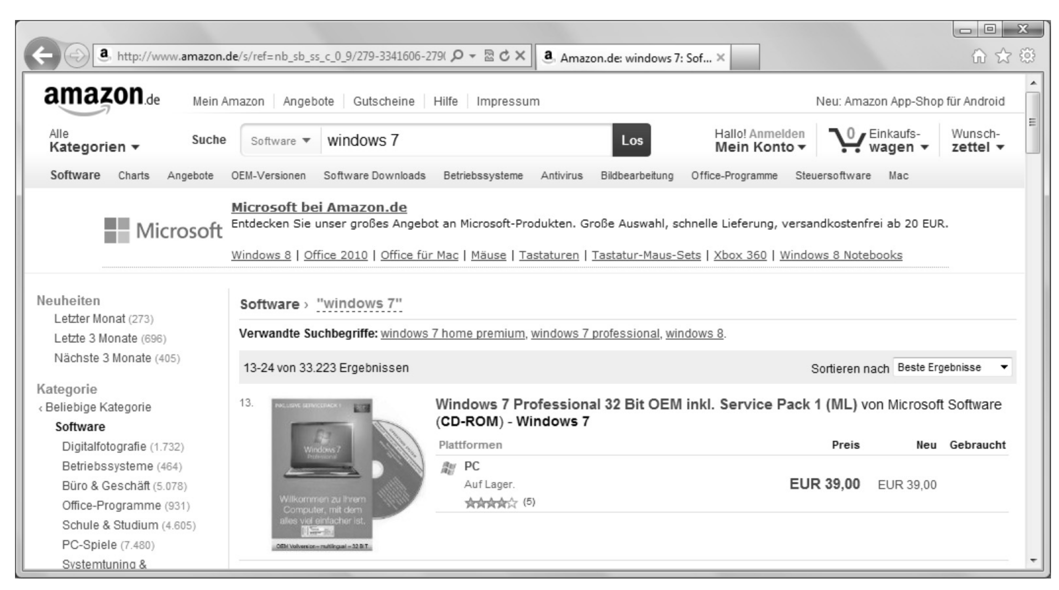


Abb. 14.1: Windows 7 mit Service Pack 1 – seinerzeit ein Bestseller!

Seit Windows 8 verzichtet Microsoft auf den Begriff »Service Pack« und verwendet nur noch den Ausdruck »Updates«, wenn Änderungen anstehen. Microsoft veröffentlichte mit Windows 8.1 nur ein großes Update, das man auch als Service Pack betrachten könnte. Es war ausschließlich über den mit Windows 8 eingeführten App Store verfügbar.

Wichtig

In der CompTIA A+-Zertifizierungsprüfung könnte es Fragen zur Installation von Updates geben. Merken Sie sich die hier genannten Schritte.

Windows Update prüft Ihr System und kann diese Updates abholen und den Rechner automatisiert patchen. Selbst wenn Sie nicht wollen, dass Windows Update automatisch Patches auf Ihrem Rechner installiert, kann es Sie immer wieder über Updates informieren, bis Sie deren Installation schließlich zustimmen. Windows Update steht in allen aktuellen Windows-Versionen zur Verfügung.

Windows Update kann automatisch ausgeführt werden, daher werden Sie wahrscheinlich beim Öffnen der App häufig neu zu installierende Updates vorfinden. Windows 7 unterscheidet drei Sorten von Updates:

- **Wichtige Updates**: Durch diese Updates werden kritische Sicherheits- oder Stabilitätsprobleme behoben. Sie können Windows Update für die automatische Installation dieser Updates konfigurieren.
- **Empfohlene Updates**: Empfohlene Updates fügen neue Funktionen hinzu oder bringen Verbesserungen mit. Sie sind nicht kritisch. Diese Updates können ebenfalls automatisch installiert werden.
- **Optionale Updates**: Hierbei handelt es sich um Gerätetreiber, Sprachpakete oder ähnliche, nicht ausschlaggebende Aktualisierungen. Optionale Updates müssen manuell installiert werden.

Wichtig

Windows Update aktualisiert nur das Betriebssystem und die Gerätetreiber. Die Firmware – BIOS oder UEFI – bleibt unangetastet.

Abbildung 14.2 zeigt Windows Update in Windows 7. Beachten Sie, dass es sich bei dem wichtigen Update um Windows 7 Service Pack 1 handelt.

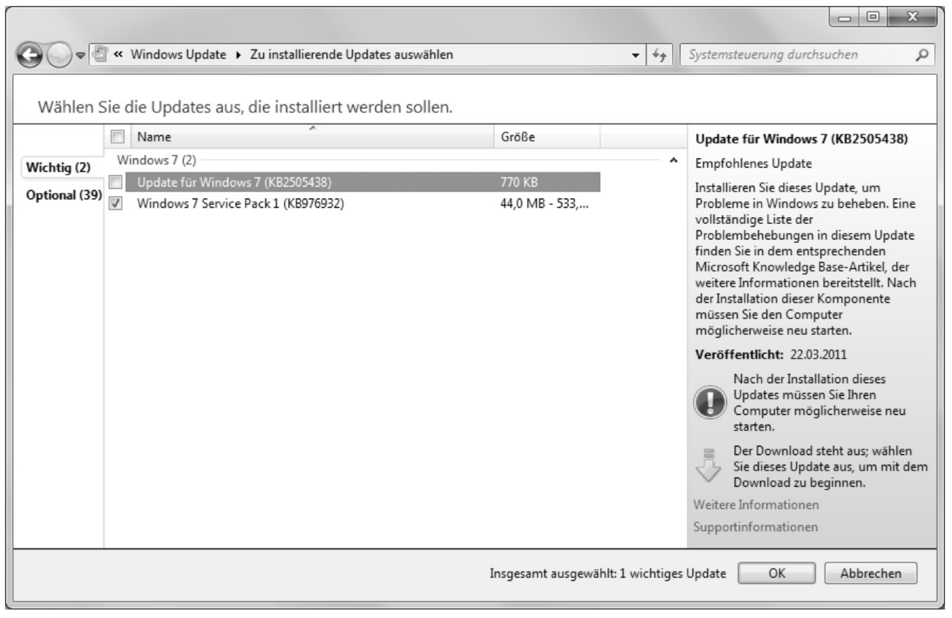


Abb. 14.2: Windows Update in Windows 7

Zum Installieren eines Updates müssen Sie dieses lediglich auswählen und auf OK klicken. Wenn Sie ein bestimmtes Update *nicht* installieren möchten und nicht immer wieder damit konfrontiert werden wollen, wenn Sie Windows Update öffnen, dann können Sie es verbergen. Klicken Sie mit der rechten Maustaste darauf und wählen Sie UPDATE AUSBLENDEN (Abbildung 14.3).

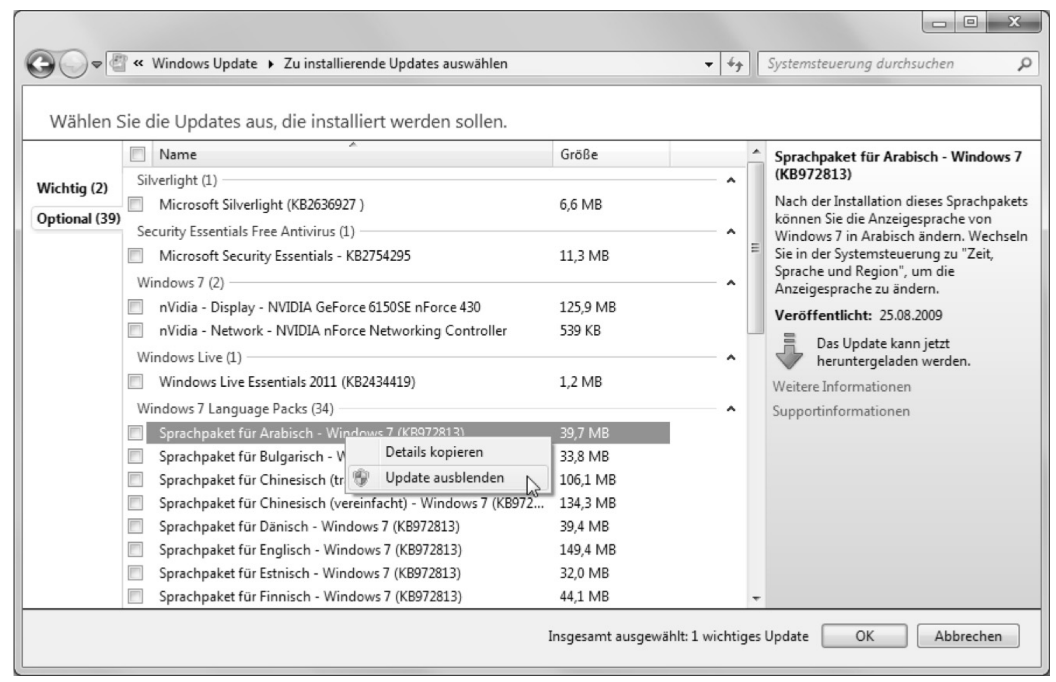


Abb. 14.3: Ausblenden eines Updates

Hinweis

In Windows 10 ist voreingestellt, dass alle Updates automatisch heruntergeladen und installiert werden. Es ist nicht mehr möglich, einzelne Updates zum Herunterladen auszuwählen.

In Windows 8 erhielt Windows Update mit der App PC-EINSTELLUNGEN einen neuen Anstrich. Die App ist im Gegensatz zum klassischen Applet der Systemsteuerung mit ihren kleinen Schaltflächen besser für berührungsempfindliche Bildschirme geeignet, bietet aber Zugriff auf die gleichen Optionen (Abbildung 14.4).

Glücklicherweise wurde das Applet WINDOWS UPDATE in der Systemsteuerung nicht durch die App PC-EINSTELLUNGEN ersetzt. Abbildung 14.5 zeigt Windows Update in Windows 7; vergleichen Sie das mit Windows Update in Windows 8.1 in Abbildung 14.6 und beachten Sie die große Ähnlichkeit.

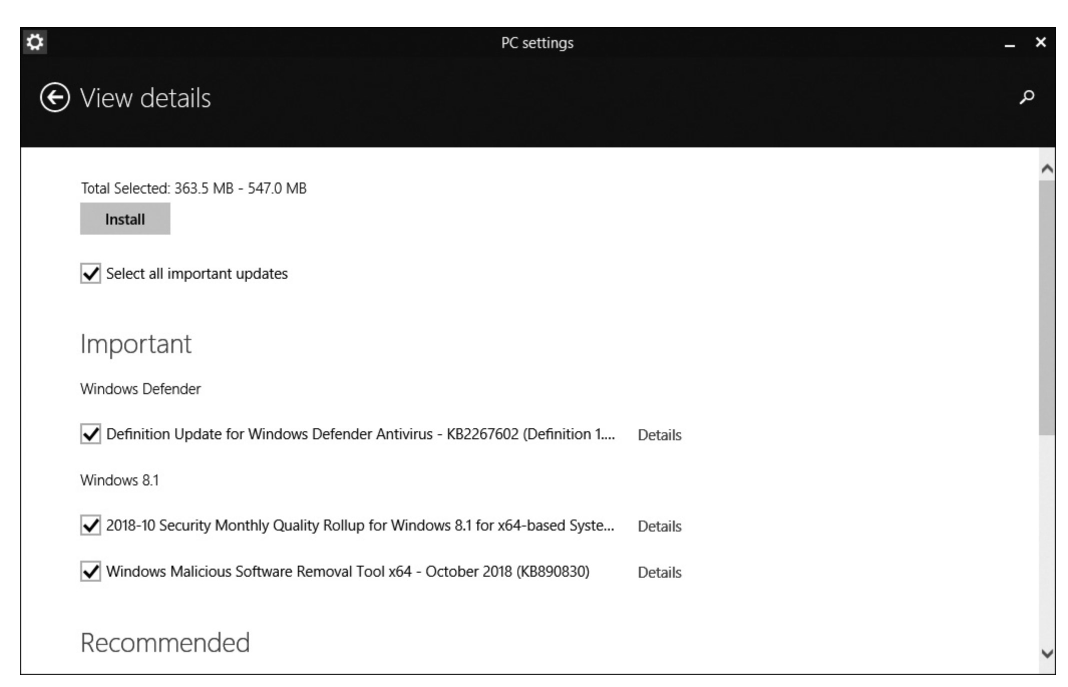


Abb. 14.4: Windows Update auf einem englischen System

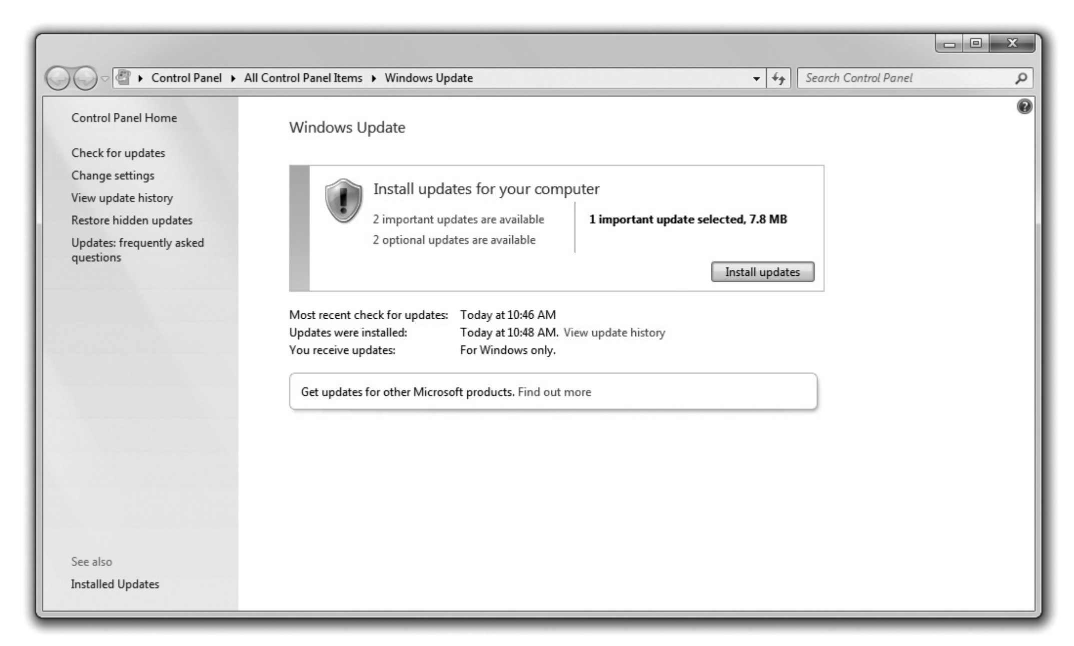


Abb. 14.5: Windows Update in der Systemsteuerung von Windows 7

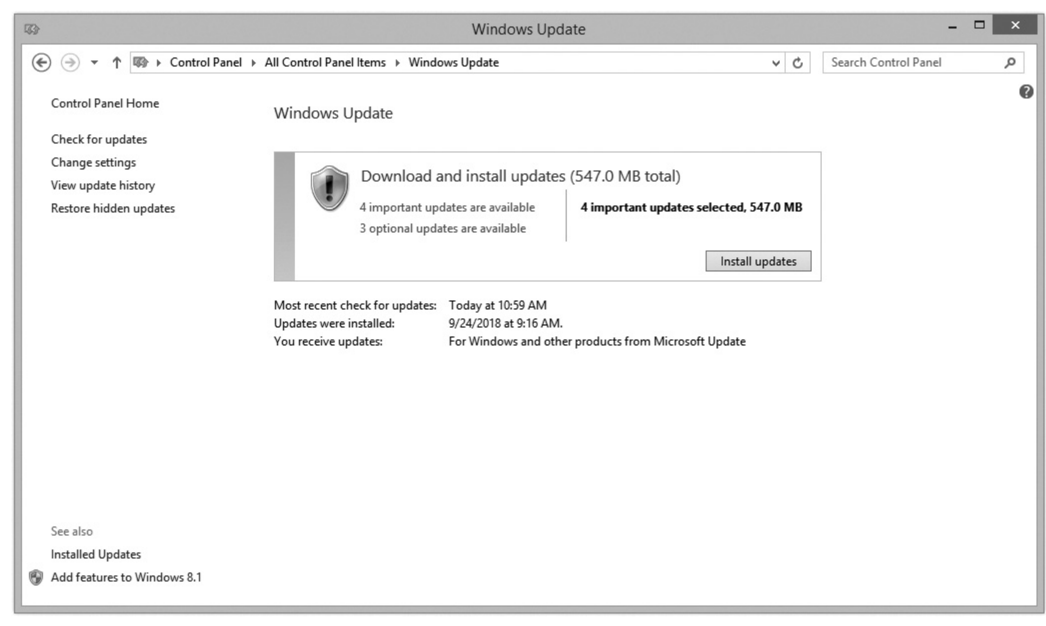


Abb. 14.6: Das Applet WINDOWS UPDATE in Windows 8.1

Sie können die installierten Updates einsehen, indem Sie auf UPDATEVERLAUF ANZEIGEN klicken. Zum Entfernen eines Updates wird das Applet PROGRAMME UND FEATURES in der Systemsteuerung benötigt. Klicken Sie links auf INSTALLIERTE UPDATES ANZEIGEN, um den Bildschirm UPDATES DEINSTALLIEREN anzuzeigen (Abbildung 14.7).

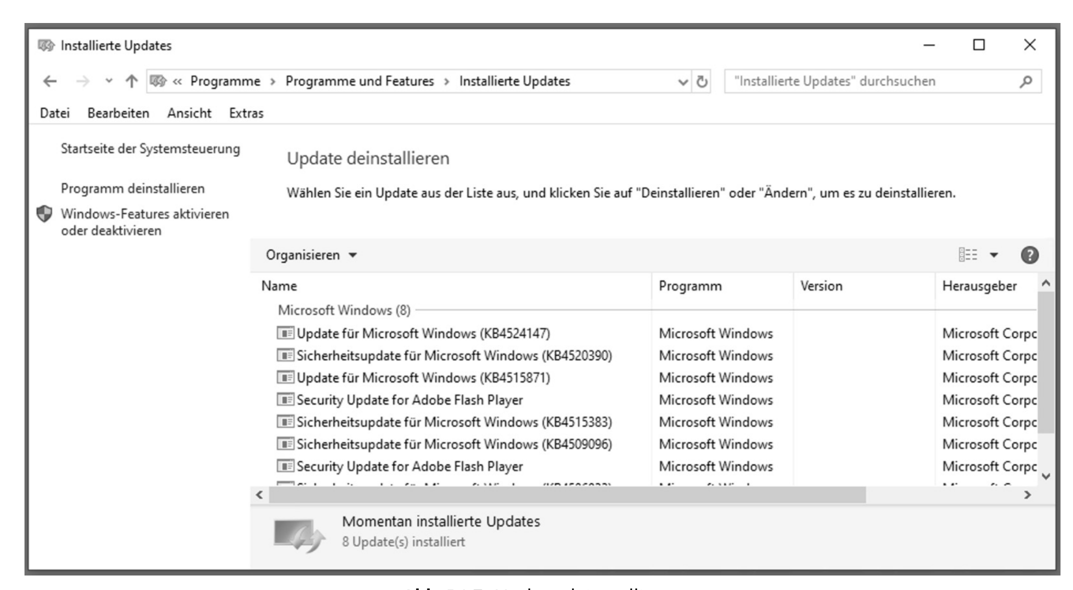


Abb. 14.7: Update deinstallieren

Die Änderungen an Windows Update in Windows 8 hatten eher kosmetischen Charakter, aber in Windows 10 wurden einige bedeutende strukturelle Änderungen vorgenommen. In Windows 10 gibt es in der Systemsteuerung kein Applet für Windows Update. Wenn Sie Änderungen vornehmen möchten, müssen Sie in den Einstellungen WINDOWS UPDATE aufrufen (Abbildung 14.8). Zwei Dinge fehlen.

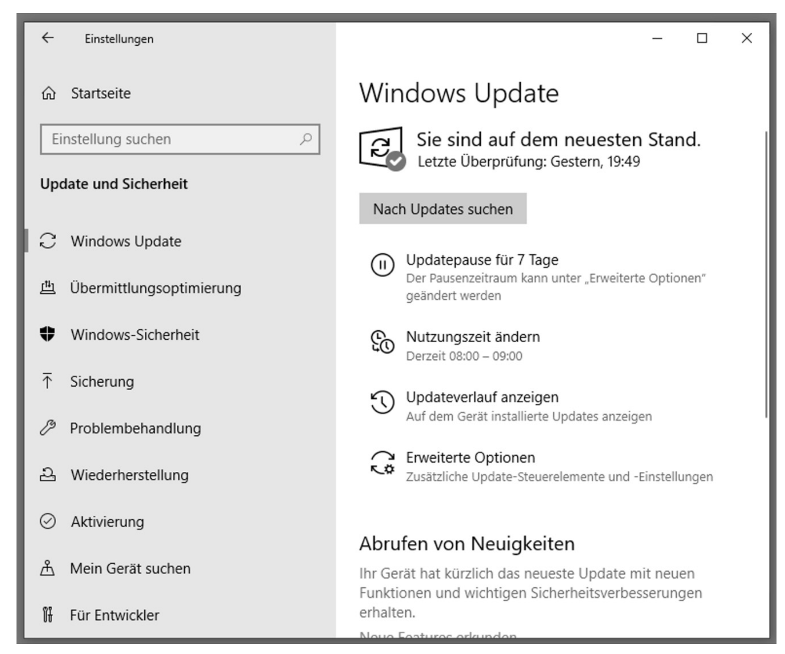


Abb. 14.8: WINDOWS UPDATE in Windows 10

Erstens können Einzelbenutzer Windows Update nicht abschalten, das gehört zum Geschäftsmodell *Windows as a Service*, das Microsoft bei Windows 10 nutzt. Der Benutzer kann Updates bis zu 35 Tage aufschieben, kann Updates jedoch nicht überspringen oder verbergen. Immerhin hat der Benutzer die Möglichkeit, die Nutzungszeit zu ändern, um Windows mitzuteilen, wann es zwecks Installation der neuesten Updates neu starten kann.

Zweitens gibt es in Windows 10 die Unterscheidung zwischen wichtigen, empfohlenen und optionalen Updates nicht mehr. Stattdessen gibt es jetzt sogenannte *Qualitäts- und Funktionsupdates*. Qualitätsupdates entsprechen den klassischen Patches, allerdings mit dem Unterschied, dass sie jetzt kumulativ sind. Alle Updates enthalten sämtliche Änderungen der vorangegangenen Updates. Dadurch soll die mit dem Aktualisieren, neu Starten und erneutem Aktualisieren verbundene Plackerei verringert werden, wenn man Windows von Grund auf installiert.

Funktionsupdates hingegen sind etwas völlig Neues. Bei diesen »Updates« handelt es sich de facto um neue Windows-Versionen, die zweimal jährlich in Herbst und im Frühling veröffentlicht werden. Hier folgt eine Liste der entscheidenden Dinge, die Sie über Funktionsupdates wissen müssen.

- Es handelt sich um eine erneute Installation von Windows.
- Sie werden nach Jahr und Monat der Veröffentlichung benannt, also beispielsweise 1703, 1709, 1803 und 1809. Es gibt aber auch Marketingbezeichnungen, wie *Creators Update* oder *Oktober 2018 Update*.
- Die Verteilung hängt davon ab, über welchen Vertriebskanal Sie Windows beziehen: als Insider, über den halbjährlichen Kanal (gezielt), über den halbjährlichen Kanal oder als Long-Term Servicing Branch. Letzteres ist nur bei Unternehmenslizenzen verfügbar.

Benutzer können Windows-Updates also nicht verhindern. Sie können aber Updates, die nicht zum System gehören, wie in Windows 7 und Window 8/8.1 deinstallieren, wenn sie in der Systemsteuerung PROGRAMME UND FEATURES aufrufen und INSTALLIERTE UPDATES ANZEIGEN auswählen.

14.1.2 Patchverwaltung in macOS und Linux

Sowohl macOS als auch Linux können Sie automatisch benachrichtigen, wenn Softwareaktualisierungen vorliegen. In älteren macOS-Versionen können Sie über die Systemeinstellung APP STORE auf Updates zugreifen, neuere Versionen verwenden die Systemeinstellung SOFTWAREUPDATES (Abbildung 14.9). Die meisten für Desktops vorgesehenen Linux-Distributionen bringen ein Werkzeug zur Softwareaktualisierung mit, das demjenigen von Ubuntu (Abbildung 14.10) ähnelt.



Abb. 14.9: Systemeinstellung SOFTWAREUPDATES

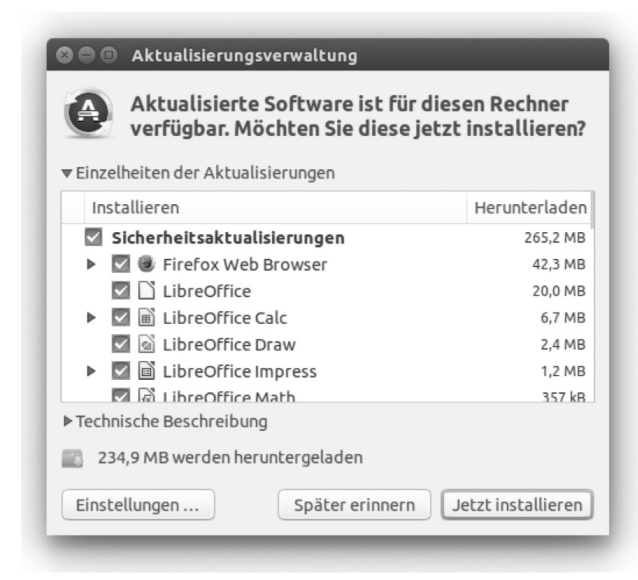


Abb. 14.10: Aktualisierungsverwaltung in Ubuntu

14.1.3 Temporäre Dateien und Datenträgerbereinigung

Vergessen Sie nicht die gelegentliche *Datenträgerbereinigung*, um die überflüssigen Dateien zu entfernen, die sich bei der täglichen Arbeit ansammeln. Wenn Sie in der Nacht durch das Web surfen, kostet das nicht nur Zeit, sondern auch Speicherplatz, weil Hunderte temporärer Internetdateien zurückbleiben. Diese und andere Relikte, wie beispielsweise »gelöschte« Dateien, die sich immer noch in Ihrem Papierkorb befinden, können jede Menge Festplattenspeicher belegen, wenn Sie diese nicht regelmäßig entfernen.

Hinweis

In der jüngsten Version von Windows 10 gibt es ein Feature namens *Speicheroptimierung*, das Sie anstelle der Datenträgerbereinigung verwenden können, das ältere Werkzeug ist aber auch noch verfügbar. Die Datenträgerbereinigung gehört nur zur CompTIA A+-Prüfung, weil die Lernziele vor dem Wechsel auf Speicheroptimierung erschienen sind. Die Speicheroptimierung entfernt automatisch überflüssige Dateien.

Wenn Sie im EIGENSCHAFTEN-Dialogfeld eines Datenträgers auf der Registerkarte ALLGEMEIN auf BEREINIGEN klicken, berechnet die Datenträgerbereinigung den Platz, der wahrscheinlich freigegeben werden kann, und zeigt anschließend ein Dialogfeld an. Darin wird angegeben, wie viel Speicherplatz durch das Löschen bei den einzelnen Kategorien und insgesamt gewonnen werden kann. Beim Start des Programms können Sie zusätzlich festlegen, ob Sie nur die eigenen Dateien oder alle Dateien auf dem Rechner bereinigen wollen. In Abbildung 14.11 sind nur einige wenige Kategorien in der Liste der zu löschenden Dateien aktiviert, daher wird natürlich weniger Platz freigegeben als ursprünglich geschätzt. Während der Aus- und Abwahl der Kategorien können Sie beobachten, wie sich die Menge des freigegebenen Speicherplatzes verändert.

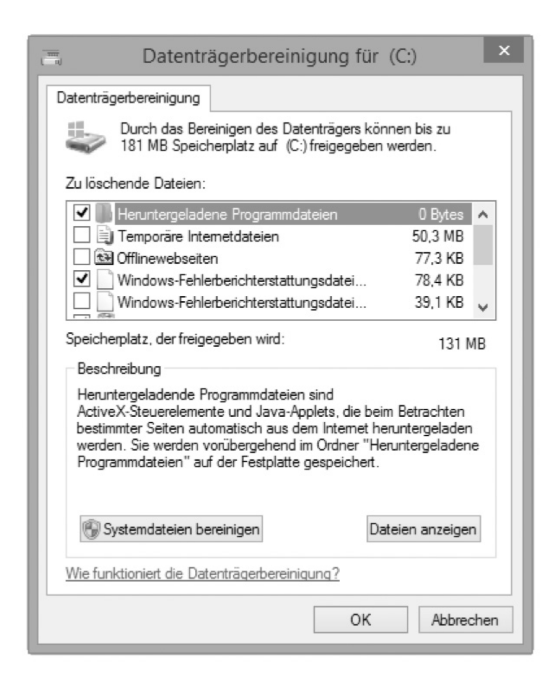


Abb. 14.11: Das Dialogfeld DATENTRÄGERBEREINIGUNG

Wenn Sie sich in der Liste nach unten bewegen, stoßen Sie auf die Möglichkeit zur Komprimierung alter Dateien. Überraschenderweise scheint die Datenträgerbereinigung mehr zu machen, als nur

Dateien zu löschen. Hier erhalten Sie einige der wenigen Möglichkeiten zur Rückgewinnung größerer Mengen an Speicherplatz. Eine weitere Kategorie, mit der Sie im größeren Rahmen Speicherplatz sparen können, finden Sie bei den temporären Internetdateien. Probieren Sie die Datenträgerbereinigung einmal auf einem Computer aus, der täglich mehrere Stunden zum Surfen im Internet genutzt wird – Sie werden mit dem Ergebnis sehr zufrieden sein!

Hinweis

Dass Sie Festplattenplatz zurückgewinnen können, bedeutet nicht, dass die Datenträgerbereinigung völlig umsonst zu haben ist. Wenn Sie viele der Kategorien auswählen, wie beispielsweise die Miniaturansichten, kann das zur Folge haben, dass Ihr Computer etwas langsamer arbeitet, bis Windows diese Cachedateien wieder erstellt hat.

14.1.4 Wartung der Registry

Ihre Registry ist eine riesige Datenbank, die Windows ständig aktualisiert, wenn Sie neue Programme oder Hardware installieren oder Änderungen daran vornehmen. Aus diesem Grund ist sie häufig voll mit Einträgen, die längst nicht mehr relevant sind. Diese Einträge verursachen normalerweise keine direkten Probleme, aber sie können Ihr System bremsen. Interessanterweise bietet Microsoft kein Werkzeug zur Bereinigung der Registry. Um die Registry zu bereinigen, brauchen Sie ein Programm von einem Drittanbieter. Für diesen Zweck gibt es eine ganze Reihe von Programmen. Mein Favorit ist die Freeware *CCleaner* von Piriform (Abbildung 14.12). Die aktuelle Version können Sie unter `www.piriform.com/ccleaner/` herunterladen. (Achten Sie beim Download und der Installation darauf, dass Sie keine zusätzlichen Programme installieren, sondern nur die kostenlose Version – es sei denn, Sie möchten den technischen Support von Piriform in Anspruch nehmen. Dann sollten Sie das Unternehmen auf jeden Fall finanziell unterstützen.)

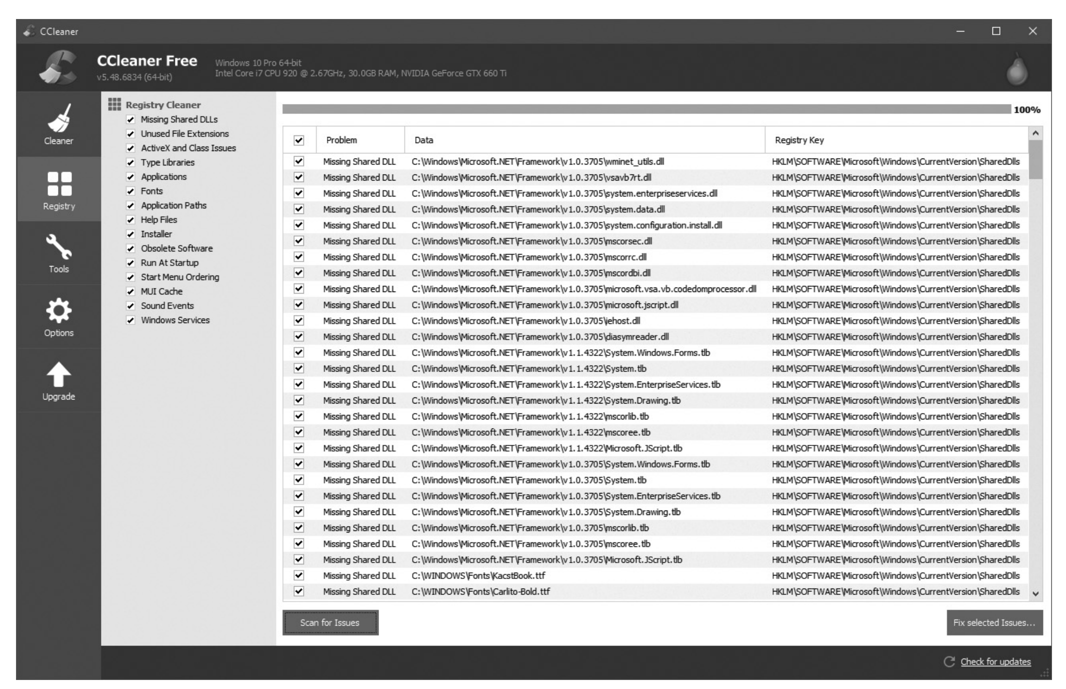


Abb. 14.12: CCleaner

Bevor Sie nun in wilden Aktionismus verfallen und anfangen, Ihre Registry zu bereinigen, sollten Sie beachten, dass alle Bereinigungswerkzeuge ein gewisses Risiko bergen, weil immer die Gefahr besteht, dass etwas aus der Registry gelöscht wird, was noch benötigt wird. Da sich die Registry zwischen den verschiedenen Windows-Versionen unterscheidet, müssen Sie darauf achten, dass Ihr Dienstprogramm die eingesetzte Windows-Version auch wirklich unterstützt. Das gilt insbesondere für die 64-Bit-Versionen von Windows!

Hinweis

Viele der Programme zum Aufräumen der Registry bereinigen auch gängige Webbrowser oder andere verbreitete Anwendungen.

14.1.5 Wartung von Laufwerken

Alle modernen Betriebssysteme bringen Werkzeuge zur Wartung von Festplattenlaufwerken und SSDs mit. Allerdings ist dabei in Windows etwas mehr Aufwand erforderlich, als in macOS und Linux. Wir betrachten alle drei Systeme.

Wichtig

Die Leistung betreffende Prüfungsfragen werden sich wahrscheinlich auf die in den Lernzielen aufgeführten Werkzeuge der verschiedenen Betriebssysteme beziehen. Sie sollten also wissen, welches Werkzeug in einer bestimmten Situation einzusetzen ist, wo Sie es finden und wie Sie damit das gewünschte Ergebnis erzielen.

Fehlerprüfung und Defragmentierung in Windows

Laufwerke gesund und munter zu halten, ist eine entscheidende Aufgabe für jeden Techniker. Die *Fehlerprüfung* und die *Defragmentierung*, um die es in Kapitel 9, *Vorbereitung und Wartung von Festplatten*, ging, sind unter Windows die wichtigsten Wartungswerkzeuge für diese Aufgabe.

Wenn Sie für ein Problem wie einen Systemabsturz oder einen Neustart keine Gründe in der Software finden (und da gibt es viele Möglichkeiten), könnte das physische Massenspeichergerät die Ursache sein. Um dies festzustellen, setzen Sie die Fehlerprüfung ein. Die Fehlerprüfung kann mit dem Befehl `chkdsk` von der Eingabeaufforderung mit erhöhten Rechten aus erfolgen. Sie können aber auch über die grafische Benutzeroberfläche auf das Werkzeug zugreifen, wenn Sie das zu prüfende Laufwerk mit der rechten Maustaste anklicken, EIGENSCHAFTEN wählen und dann die Registerkarte TOOLS aktivieren, auf der Sie die Schaltfläche JETZT PRÜFEN bzw. PRÜFEN (je nach Betriebssystemversion) anklicken. Dann durchsucht die Fehlerprüfung das Laufwerk nach Fehlern im Dateisystem und versucht, sie – falls möglich – zu reparieren (Abbildung 14.13).

Die Defragmentierung (Windows 7) oder Laufwerke optimieren (Window 8 und neuer) verhindert, dass Ihr System langsam wird, indem sie die in vielen kleinen Teilen über die ganze Festplatte verteilten Dateien in einzelne zusammenhängende Dateien umorganisiert (Abbildung 14.14). Alle aktuellen Windows-Versionen führen die Defragmentierung von plattenbasierten Laufwerken automatisch durch. Bei SSDs ist eine Defragmentierung nicht erforderlich. Klicken Sie mit der rechten Maustaste auf ein Laufwerk und wählen Sie EIGENSCHAFTEN. Klicken Sie dann auf der Registerkarte TOOLS auf JETZT DEFRAGMENTIEREN bzw. auf OPTIMIEREN, um das Werkzeug aufzurufen.



Abb. 14.13: Fehlerüberprüfung in Windows 10

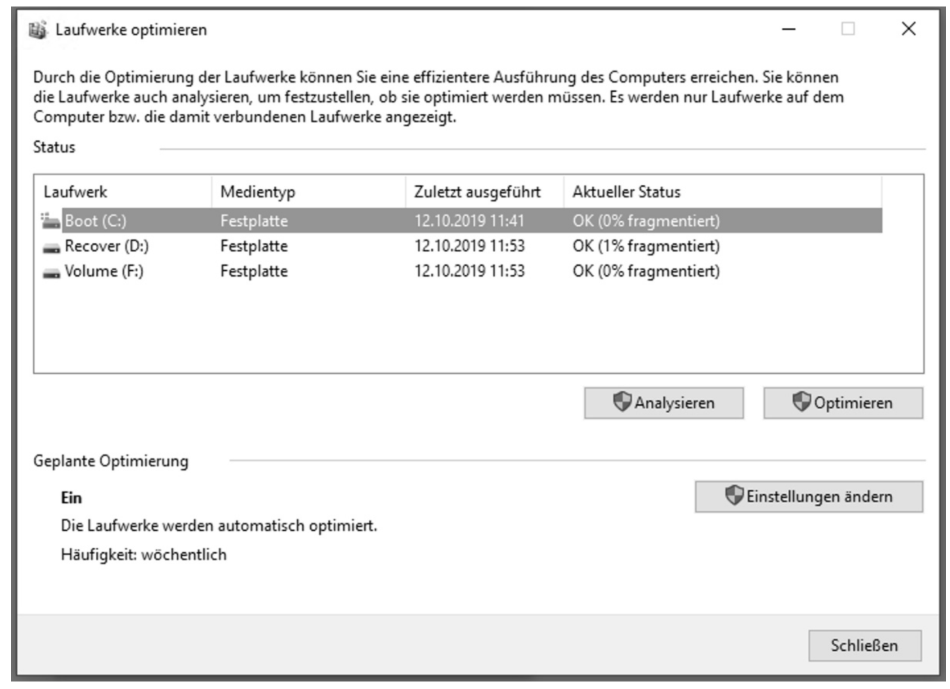


Abb. 14.14: Laufwerke optimieren in Windows 10

Die Fehlerprüfung und die Defragmentierung sind derart wichtige Wartungsprogramme, dass Sie diese wirklich automatisch ausführen lassen sollten. Werfen wir nun einen Blick auf macOS und Linux. Danach sehen wir uns an, wie wir diese und andere kritische Aufgaben geplant ausführen lassen können.

Hinweis

SSDs werden auf völlig andere Art und Weise optimiert als HDDs. Glücklicherweise wissen alle Betriebssysteme damit umzugehen und handhaben die Optimierung von Laufwerken verschiedenen Typs automatisch.

Festplattendienstprogramm in macOS

macOS erledigt die Wartungsaufgaben von Laufwerken, wie Windows auch, automatisch. Wenn Sie eine Fehlerüberprüfung eines Laufwerks durchführen möchten, stellt macOS das Festplattendienstprogramm bereit, ein Werkzeug zur Wartung von Festplatten, das zum Überprüfen und Reparieren der Dateistrukturen verwendet wird. Die aktuelle Version des Festplattendienstprogramms erlaubt es außerdem, Laufwerke zu partitionieren und andere Wartungsarbeiten zu erledigen. Wählen Sie ein Laufwerk aus und klicken Sie auf ERSTE HILFE, um ein Laufwerk zu überprüfen.

Optionen unter Linux

Praktisch jede Linux-Distribution bringt Werkzeuge zur Wartung von Laufwerken mit. Darüber hinaus stehen jede Menge wirklich gute Anwendungen zum kostenlosen Herunterladen zur Verfügung. Für die meisten Techniker dürfte das Werkzeug zur Festplattenanalyse auf der Installations-DVD das Mittel der Wahl sein. Starten Sie einfach den Rechner mit eingelegtem Installationsmedium neu. Bei manchen Installations-Discs oder USB-Speichersticks erscheint dann ein Tastatursymbol auf dem Bildschirm. Wenn Sie dann ↵ drücken, werden Optionen zum Überprüfen von Laufwerken, Testen des Arbeitsspeichers usw. angezeigt (Abbildung 14.15). Eine weitere Möglichkeit besteht darin, sich mit der *Ultimate Boot CD* ein Rundum-glücklich-Paket herunterzuladen. Sie finden es unter `www.ultimatebootcd.com`.



Abb. 14.15: Die Optionen bei der Installation von Ubuntu

14.1.6 Geplante Ausführung von Wartungsarbeiten

Die Wartung kann nur dann richtig funktionieren, wenn sie regelmäßig ausgeführt wird. Abhängig von der jeweiligen Windows-Version können Sie verschiedene Wartungsarbeiten automatisch nach einem Zeitplan ausführen lassen. Innerhalb der Prüfungsziele der CompTIA gibt es zwei Bereiche, die sich dafür anbieten: Datensicherung und Datenträgerprüfung (Fehlerprüfung).

Windows: Aufgabenplanung

Aktuelle Windows-Versionen verwenden zur geplanten Ausführung von Wartungsarbeiten ein Werkzeug namens *Aufgabenplanung*. Damit können Sie ein ausführbares Programm auswählen und festlegen, wann es ausgeführt werden soll. Entscheidend ist, dass Sie den Namen und die erforderlichen Parameter des Programms kennen, das Sie ausführen möchten.

Aufgaben werden in Trigger, Aktionen und Bedingungen unterteilt. *Trigger* (*Auslöser*) sind Aktionen oder Zeitpunkte, die den Start eines Programms auslösen. *Aktionen* sind Schritte, die definieren, welches Programm wie ausgeführt werden soll. *Bedingungen* sind zusätzliche Kriterien, die erfüllt sein müssen, wenn das Programm ausgeführt werden soll. (Befindet sich das System im Leerlauf? Ist es mit dem Internet verbunden?) Abbildung 14.16 zeigt die Registerkarte BEDINGUNGEN für eine geplante Defragmentierung. Um eine Aufgabe einzurichten, müssen Sie ihr lediglich eine Bezeichnung geben, einstellen, wie oft sie ausgeführt werden soll und festlegen, was sie tut.

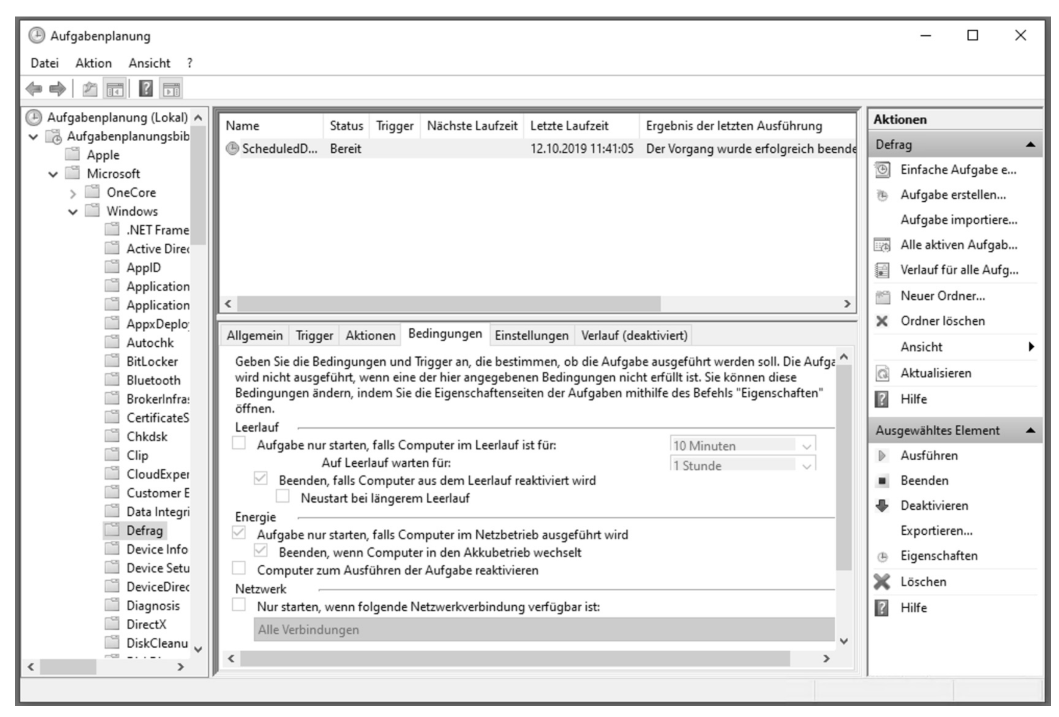


Abb. 14.16: Die Registerkarte BEDINGUNGEN in der AUFGABENPLANUNG

Viele Windows-Dienstprogramme bieten die Möglichkeit, Aufgaben zu planen. Diese Programme bedienen sich ebenfalls der AUFGABENPLANUNG, allerdings verhindert Windows das Bearbeiten der Einträge vieler dieser Programme. Sie können beispielsweise in der AUFGABENPLANUNG einen Eintrag für die automatische Defragmentierung sehen. Um ihn zu bearbeiten, müssen Sie jedoch in LAUF-

WERKE OPTIMIEREN über die Schaltfläche EINSTELLUNGEN ÄNDERN ein entsprechendes Dialogfeld öffnen (Abbildung 14.17).

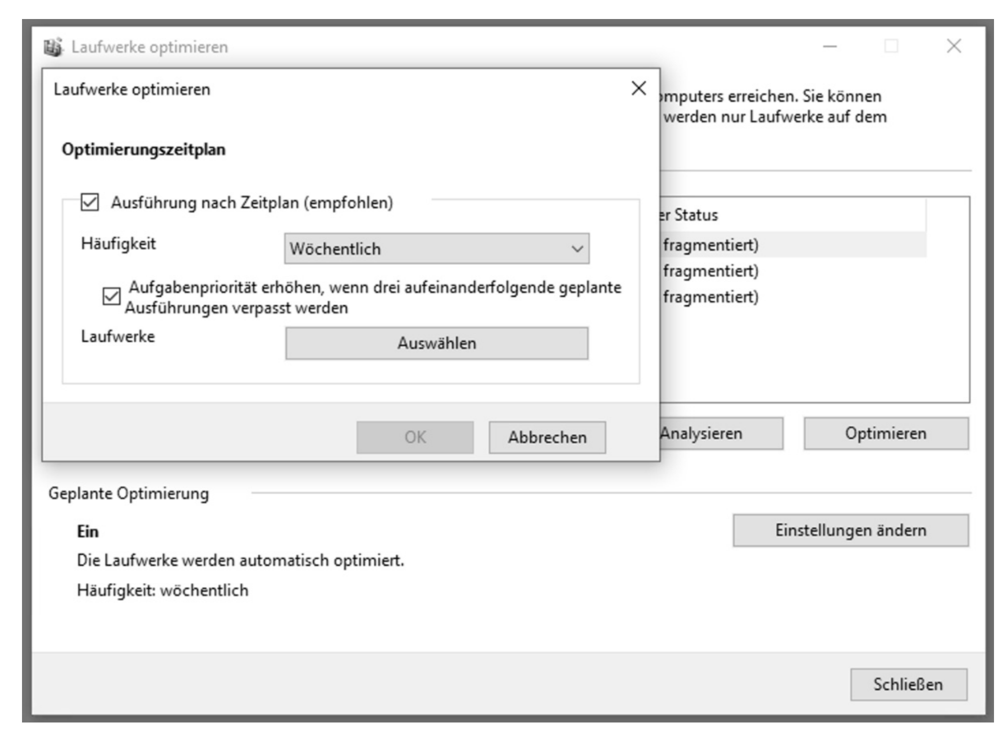


Abb. 14.17: Aufgabenplanung für LAUFWERKE OPTIMIEREN

macOS und Linux: launchd und cron

macOS und die meisten Linux-Distributionen nutzen eines von zwei Werkzeugen zur Skriptausführung, um die verschiedensten Aufgaben automatisch im Hintergrund auszuführen. Apple hat zur Automatisierung den *launchd* (sprich: Launch-Dämon) entwickelt. Die meisten Linux-Distributionen verwenden hingegen das etwas universellere und ältere *cron*. Sie können problemlos eigene launchd- und cron-Jobs einrichten, die Einzelheiten gehen jedoch weit über das für die CompTIA A+-Zertifizierungsprüfungen erforderliche Wissen hinaus, daher lasse ich sie weg. Sie sollten sich die Bezeichnungen aber merken.

Wichtig

In macOS brauchen Sie *keine* geplante Wartung der Laufwerke durchzuführen. (Tatsächlich bietet das Festplattendienstprogramm diese Möglichkeit gar nicht.) Das Betriebssystem führt regelmäßig nachts eine Überprüfung durch und behebt entweder die Probleme oder weist Sie darauf hin, wenn Sie Ihren Mac das nächste Mal verwenden.

Geplante Datensicherung in Windows

Die Sicherung kritischer Dateien ist ein wichtiger Bestandteil der Wartung eines Betriebssystems. Alle Betriebssysteme bringen irgendein Hilfsprogramm zur Datensicherung mit, um wichtige Dateien auf zusätzlichen Festplatten, auf USB-Speichersticks, über das Netzwerk oder in der Cloud zu speichern.

Je nach Windows-Version werden verschiedene Programme zur Datensicherung verwendet. In Windows 7 gibt es das Werkzeug SICHERN UND WIEDERHERSTELLEN, Windows 8/8.1/10 verwenden ein Programm namens DATEIVERSIONSVERLAUF. (Allerdings gibt es in Windows 10 ebenfalls ein Werkzeug namens SICHERN UND WIEDERHERSTELLEN.) Mehr dazu später in diesem Kapitel, zunächst möchte ich die Planung regelmäßiger Datensicherungen untersuchen, eine in Windows 7 unverzichtbare und in neueren Windows-Versionen praktische Maßnahme.

Jede Datensicherung besteht aus zwei wichtigen Schritten. Erstens wählen Sie aus, welche Dateien gesichert werden sollen. Zweitens legen Sie durch irgendeine Art der Planung fest, wann die Sicherung stattfindet. Das Applet DATEIVERSIONSVERLAUF in Windows 10 bietet ebenfalls einen Zeitplaner. Am Ende des entsprechenden Assistenten können Sie nach Auswahl der zu kopierenden Ordner und des Speichermediums die Schaltfläche ERWEITERTE EINSTELLUNGEN verwenden, um festzulegen, wann und wie oft Windows eine Datensicherung erstellen soll (Abbildung 14.18). Es ist tatsächlich so einfach.

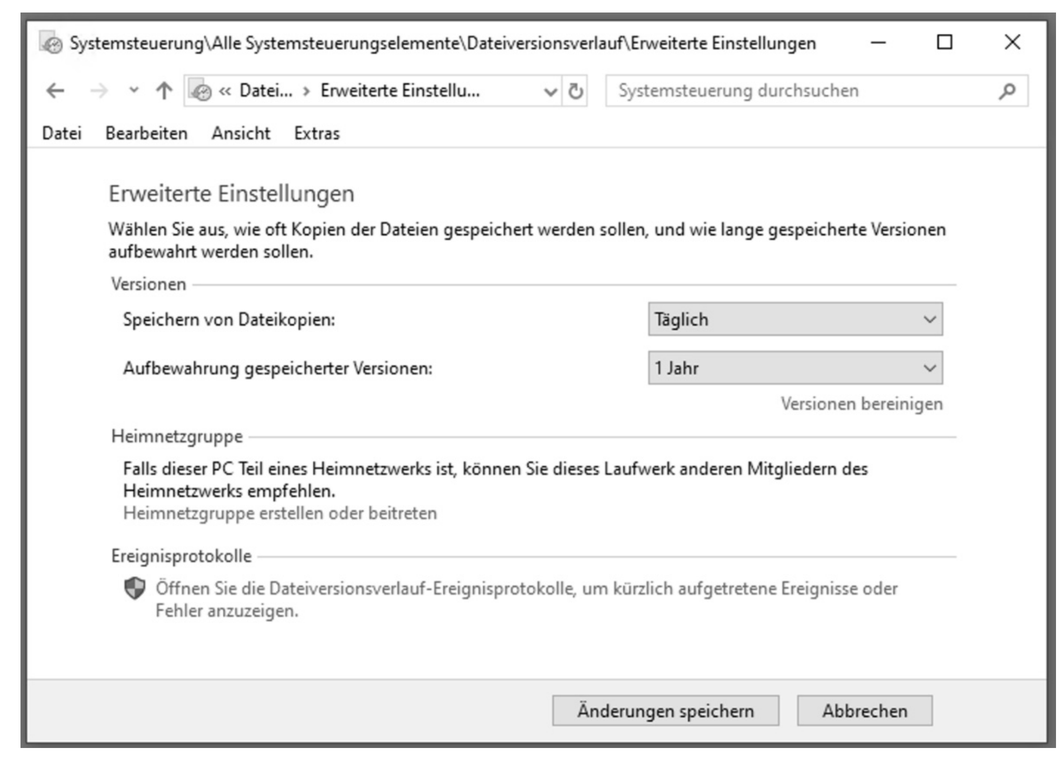


Abb. 14.18: Zeitplan für die Datensicherung

Wie oft sollte eine Datensicherung vorgenommen werden? Wenn Sie eigene Dokumente erstellen, Musik aus dem Internet herunterladen und viele digitale Fotos aufnehmen, ist eine stündliche Sicherung angebracht. Wenn Sie nur ein gelegentlicher Benutzer sind, der hin und wieder ein wenig surft und eine Runde Solitär spielt, ist eine tägliche Datensicherung möglicherweise ausreichend.

Hinweis

Wenn Sie macOS verwenden, brauchen Sie keine Planung vorzunehmen. Sobald Sie Time Machine eingerichtet haben, müssen Sie sich um nichts mehr kümmern. Mehr dazu im Abschnitt *Time Machine in macOS* weiter hinten in diesem Kapitel.

14.1.7 Autostart-Software konfigurieren

Beim Start des Computers wird jede Menge Software geladen und gestartet. Denken Sie nur an all die kleinen Programme, die zur Unterstützung der verschiedenen Funktionen des Betriebssystems dienen. Man bezeichnet sie als *Dienste*. Wenn Sie Ihrem System Anwendungen und Peripheriegeräte hinzufügen, kommt weitere Software hinzu, die beim Systemstart automatisch geladen wird. Im Allgemeinen sind diese Autostart-Programme erwünscht – schließlich soll Ihr Peripheriegerät ja ordnungsgemäß funktionieren. Manche Autostartprogramme können jedoch Probleme verursachen und müssen vorübergehend oder dauerhaft entfernt werden.

Alle Betriebssysteme bieten die Möglichkeit, den Autostart von Anwendungen, Prozessen und Diensten zu unterbinden. Unter Windows stehen dafür die Werkzeuge Systemkonfiguration und Task-Manager zur Verfügung. Apple rät von Autostartprogrammen zwar ab, aber dennoch verwendet jedes Benutzerkonto bestimmte Anmeldeobjekte, die beim Start geladen werden. Verwenden Sie in macOS die Systemeinstellung BENUTZER & GRUPPEN, um die Anmeldeobjekte zu konfigurieren. Suchen Sie in Linux (Ubuntu) mit der Suche auf dem Schreibtisch nach »Startprogramme«, um diese zu konfigurieren.

Systemkonfiguration

Techniker benutzen in Windows 7 das *Systemkonfigurationsprogramm* (das auch unter dem Namen der ausführbaren Datei `msconfig` bekannt ist) zur Bearbeitung der beim Start des Betriebssystems geladenen Prozesse und Dienste und der Behebung von Problemen, die in diesem Bereich auftreten. Seit Windows 8 können Sie diese Einstellungen im Task-Manager vornehmen.

Um das Programm SYSTEMKONFIGURATION zu starten, wählen Sie START|AUSFÜHREN, geben `msconfig` ein und klicken OK an oder drücken ↵. Je nach Einstellung der Benutzerkontensteuerung (*UAC – User Account Control*) müssen Sie möglicherweise erst noch Anmeldedaten angeben.

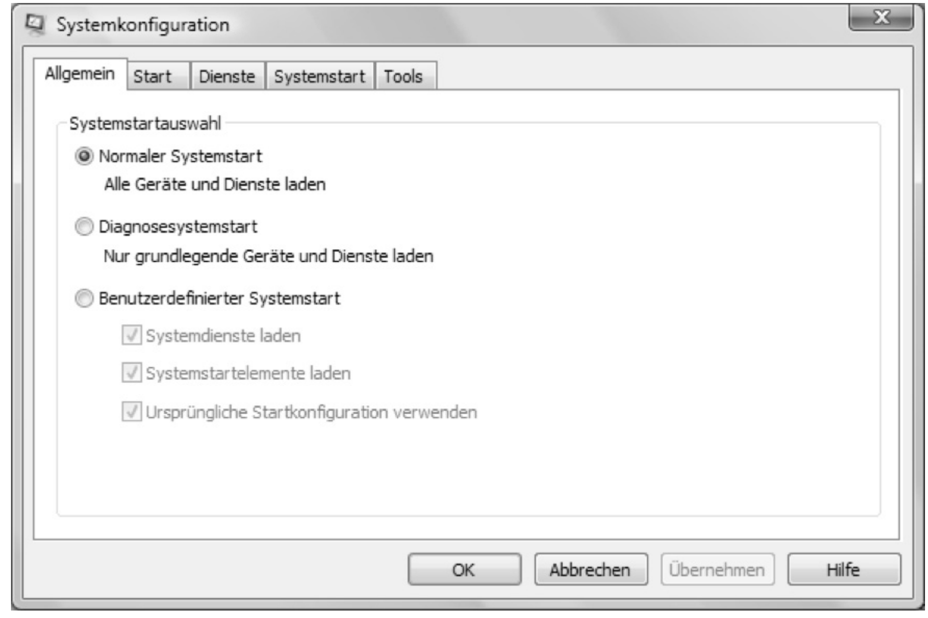


Abb. 14.19: Systemkonfiguration in Windows 7

Das Systemkonfigurationsprogramm verfügt über eine Reihe praktischer Funktionen, die auf die verschiedenen Registerkarten verteilt sind:

- **Allgemein**: Wählen Sie hier die Art des nächsten Systemstarts aus (Abbildung 14.19). Zur Auswahl stehen ein normaler Systemstart, bei dem alle Treiber geladen und Dienste gestartet werden, ein Diagnosesystemstart, bei dem nur elementare Treiber geladen und grundlegende Dienste gestartet werden, oder ein benutzerdefinierter Systemstart, bei dem Sie festlegen, ob Systemdienste und Systemstartelemente geladen werden und ob die ursprüngliche Startkonfiguration verwendet wird.
- **Start**: Hier finden sich erweiterte Funktionen für den Systemstart. Es werden alle auf dem System installierten Windows-Versionen angezeigt, Sie können ein Standard-Betriebssystem auswählen oder ein Betriebssystem aus dem Boot-Menü entfernen. Sie können hier außerdem einen sicheren Start einstellen oder erweiterte Optionen konfigurieren, wie z.B. die Anzahl der Prozessorkerne oder wie viel Arbeitsspeicher das System verwenden soll. Wenn Sie hier einen sicheren Start konfigurieren, wird Windows übrigens immer im abgesicherten Modus starten, bis Sie die Einstellung wieder ändern. Im abgesicherten Modus wird nur ein minimales allgemeines System mit bekanntermaßen funktionierenden Treibern geladen, das zur Fehlerbehebung genutzt wird. Besser ist es allerdings, F5 zu drücken, um in den abgesicherten Modus zu gelangen (nur Windows 7). Aber das sehen wir uns in Kapitel 16, *Fehlerbehebung*, noch genauer an.
- **Dienste**: Diese Registerkarte entspricht derjenigen des Task-Managers. Hier können sämtliche Dienste des PC aktiviert oder deaktiviert werden.
- **Systemstart**: Auf dieser Registerkarte können Sie Startprogramme (die beim Start von Windows ebenfalls gestartet werden) konfigurieren. Dies ist vielleicht die nützlichste der Registerkarten, insbesondere wenn Windows auf Ihrem PC langsam startet.
- **Tools**: Die Registerkarte enthält viele der in Windows verfügbaren Werkzeuge und Dienstprogramme, wie Ereignisanzeige, Leistungsüberwachung, Eingabeaufforderung usw. Sie finden hier nichts, was Ihnen in Windows nicht auch an anderer Stelle zur Verfügung steht, aber praktisch ist diese Liste allemal.

Hinweis

Das Systemkonfigurationsprogramm gibt es auch in Window 10, allerdings werden Sie nach Auswahl der Registerkarte AUTOSTART zum Task-Manager umgeleitet.

Task-Manager

In Windows 8/8.1/10 hat Microsoft die Registerkarten SYSTEMSTART (die nun AUTOSTART heißt) und DIENSTE im Task-Manager platziert. Sie können hier auf einen Blick erkennen, ob der Autostart eines Programms aktiviert oder deaktiviert ist und welche Startauswirkungen dies mit sich bringt (Abbildung 14.20). Sie können sich natürlich denken, dass ein Programm, das zuhauf Dateien über das Internet synchronisiert, größere Startauswirkungen mit sich bringt als eines, das nur lokale Dateien lädt.

Klicken Sie mit der rechten Maustaste auf einen der Einträge und wählen Sie eine der verfügbaren Optionen aus, um den Autostart eines Programms zu aktivieren oder zu deaktivieren. Beim nächsten Systemstart werden die hier vorgenommenen Einstellungen dann wirksam.

Tipp

Macht der Task-Manager Sie nervös? Dann sehen Sie sich unter `http://totalsem.com/100x` die Übung zu Kapitel 14 an, in der Sie erfahren, wie man den Task-Manager verwendet, ohne das System in Gefahr zu bringen.

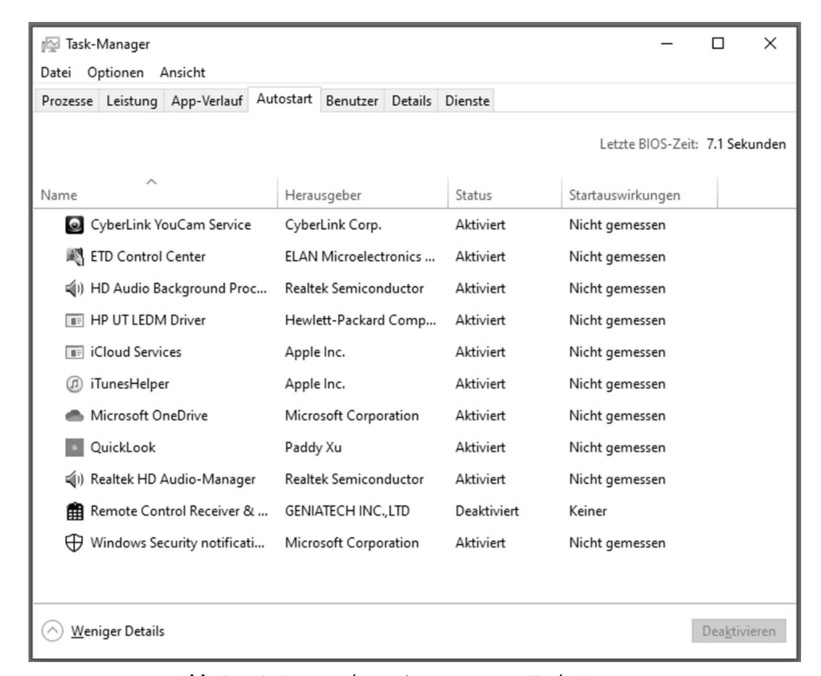


Abb. 14.20: Registerkarte AUTOSTART im Task-Manager

Benutzer & Gruppen in macOS

In der Systemeinstellung BENUTZER & GRUPPEN können Sie im Bereich ANMELDEOBJEKTE problemlos Programme hinzufügen (oder entfernen), die bei der Anmeldung eines Benutzers gestartet werden (Abbildung 14.21). Viel mehr gibt es hier nicht zu sagen, daher erlaube ich mir hier eine zusätzliche Anmerkung: macOS ist so einfach zu bedienen und zu warten, weil Apple eine extreme Kontrolle über das System ausübt.

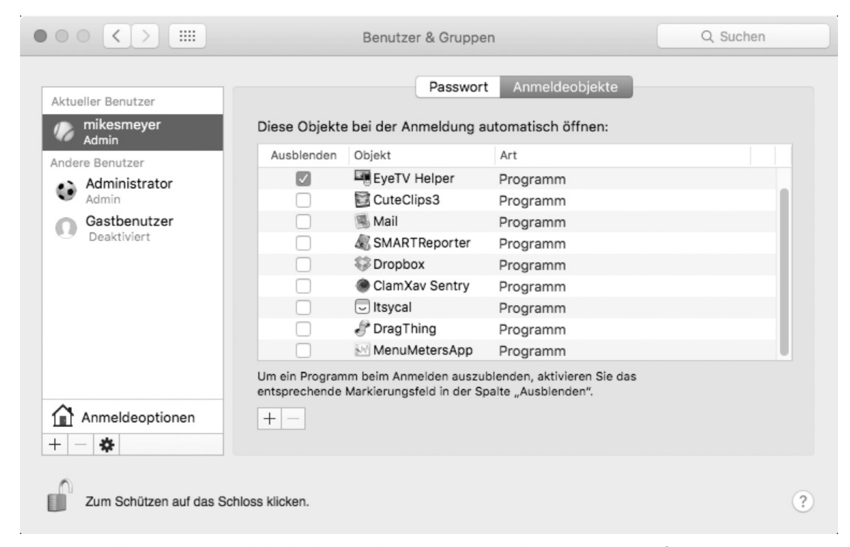


Abb. 14.21: Anmeldeobjekte in der Systemeinstellung BENUTZER & GRUPPEN

Hinweis

Wie wichtig Benutzer und Gruppen in Windows sind, haben Sie bereits in Kapitel 13 erfahren.

Startprogramme in Linux

In Ubuntu Linux können Sie auf die Startprogramme zugreifen, indem Sie danach suchen. Klicken Sie oben links auf die Schaltfläche zum Suchen und geben Sie »Startprogramme« ein. Wählen Sie das Programm unter den Suchtreffern aus, um es zu starten. Hier können Sie über die Kontrollkästchen festlegen, welche Programme beim Systemstart ebenfalls gestartet werden sollen (Abbildung 14.22).

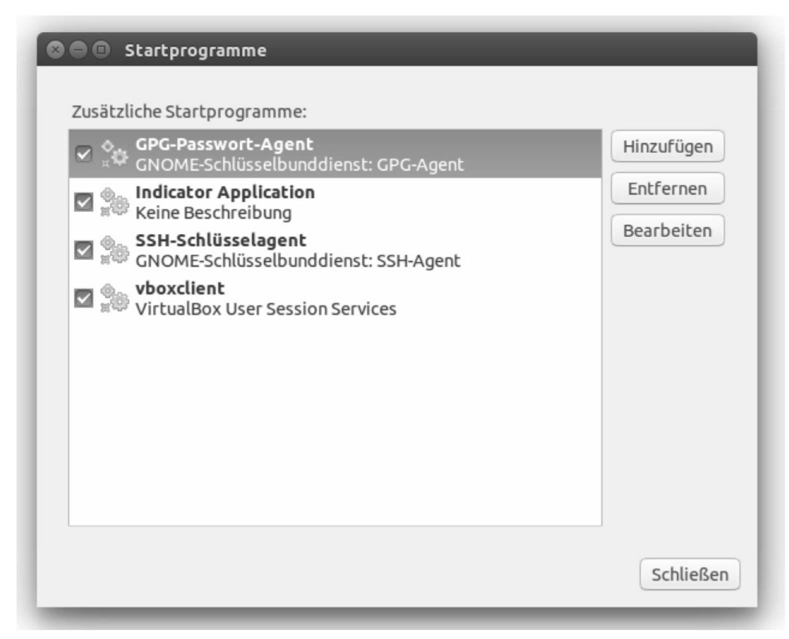


Abb. 14.22: Deaktivieren eines Autostartprogramms in STARTPROGRAMME

14.1.8 Praktische Werkzeuge zur Administration

Alle Windows-Versionen liefert Microsoft mit einigen nützlichen Werkzeugen aus. In diesem Abschnitt betrachten wir Systeminformationen und die MMC.

Systeminformationen

Zusammen mit Windows wird das praktische Werkzeug SYSTEMINFORMATIONEN ausgeliefert (Abbildung 14.23), das Information über Hardwareressourcen, Komponenten und die Softwareumgebung sammelt. Wenn es damit fertig ist, dann fasst es sie in einem netten kleinen und sauber formatierten Bericht zusammen, der Ihnen die Diagnose und Behebung aller Probleme und Konflikte erleichtert. Wie viele andere Tools erreichen Sie das Programm über START|AUSFÜHREN, denn in den CompTIA A+-Prüfungen wird auf das Tool SYSTEMINFORMATIONEN bevorzugt über seine ausführbare Datei namens `msinfo32.exe` Bezug genommen.

Wichtig ist noch anzumerken, dass Sie SYSTEMINFORMATIONEN auch dazu verwenden können, um Information über entfernte Computer zu sammeln, wenn Sie im Menü ANSICHT|REMOTECOMPUTER wählen und dann den Namen des Remotecomputers im Netzwerk eingeben.

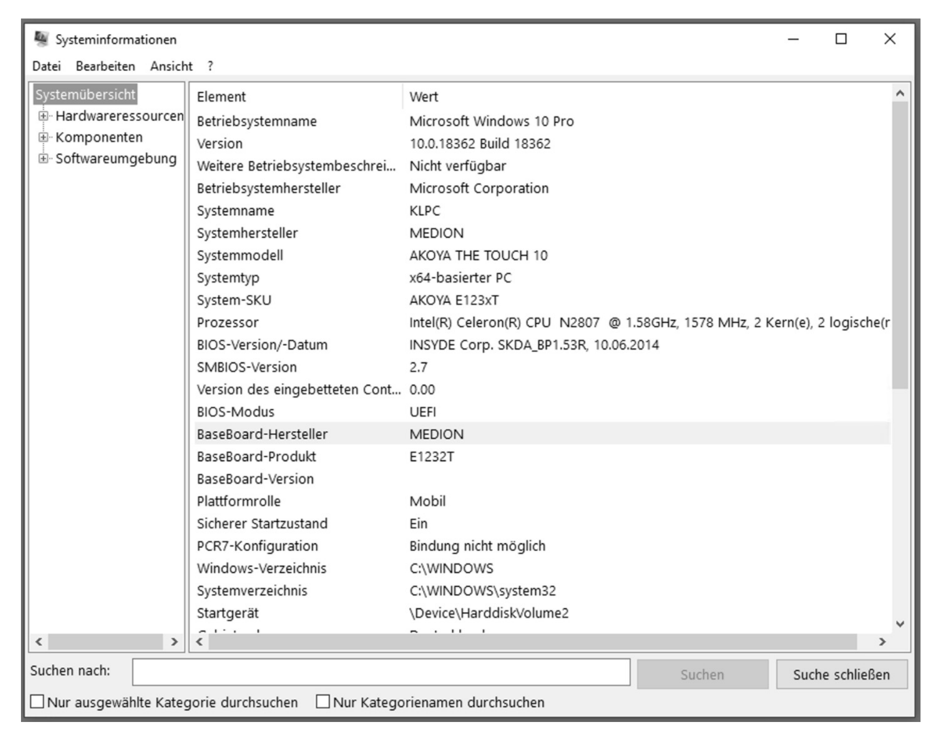


Abb. 14.23: SYSTEMINFORMATIONEN

14.1.9 Microsoft Management Console

Die *Microsoft Management Console* (MMC) ist ein Kommandozeilenprogramm, das verschiedene Hilfsprogramme zur Administration und Fehlerbehebung enthält, die *Snap-Ins* genannt werden. Die Apps in der Computerverwaltung sind beispielsweise vorkonfigurierte MMCs. Sie können für Ihren Bedarf auch benutzerdefinierte MMCs erstellen. Geben Sie in das Suchfeld `mmc` ein und drücken Sie [↵], um eine leere MMC zu öffnen. Bei einer leeren MMC gibt es allerdings nicht viel zu sehen (Abbildung 14.24).

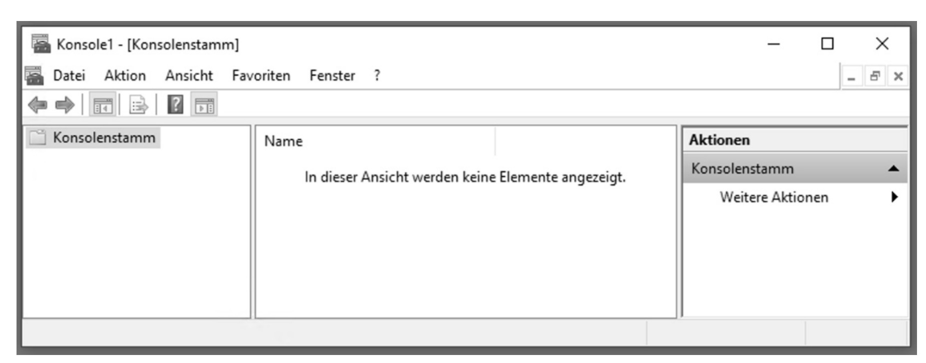


Abb. 14.24: Leere MMC

Nützlich wird eine MMC, indem Sie Snap-Ins hinzufügen, zu denen die meisten Hilfsprogramme gehören, die Sie in Windows verwenden. Sogar der Geräte-Manager ist ein Snap-In. Sie können beliebig viele Snap-Ins hinzufügen, von denen eine ganze Menge zur Auswahl stehen.

Um beispielsweise den Geräte-Manager zu der leeren MMC hinzuzufügen, wählen Sie Datei|Snap-in hinzufügen/entfernen. Im Dialogfeld Snap-Ins hinzufügen bzw. entfernen wird eine Liste der verfügbaren Snap-Ins angezeigt (Abbildung 14.25). Wählen Sie den Geräte-Manager aus, klicken Sie auf Hinzufügen und anschließend auf OK, um das Dialogfeld zu schließen. Nun sollte der Geräte-Manager in der Konsole angezeigt werden. Klicken Sie darauf. Was jetzt angezeigt wird, sollte Ihnen bekannt vorkommen (Abbildung 14.26).

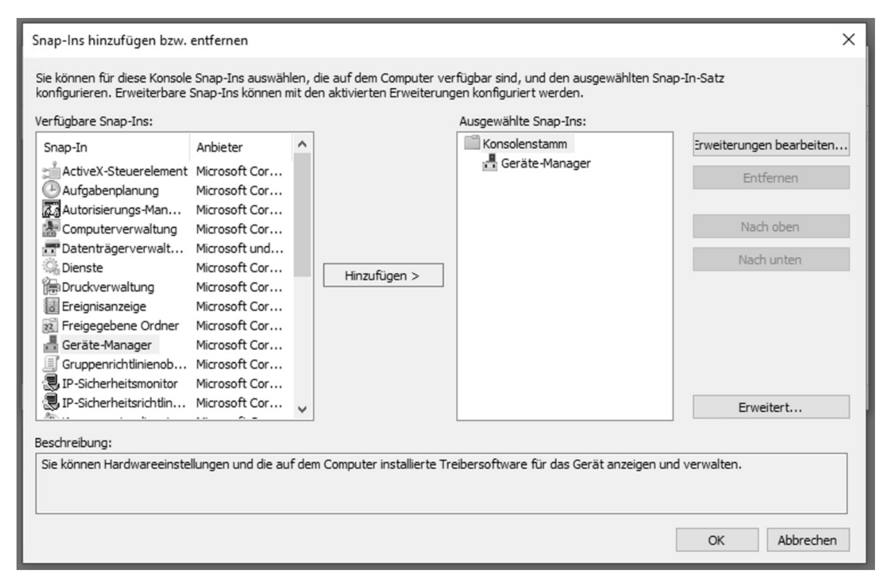


Abb. 14.25: Verfügbare Snap-Ins

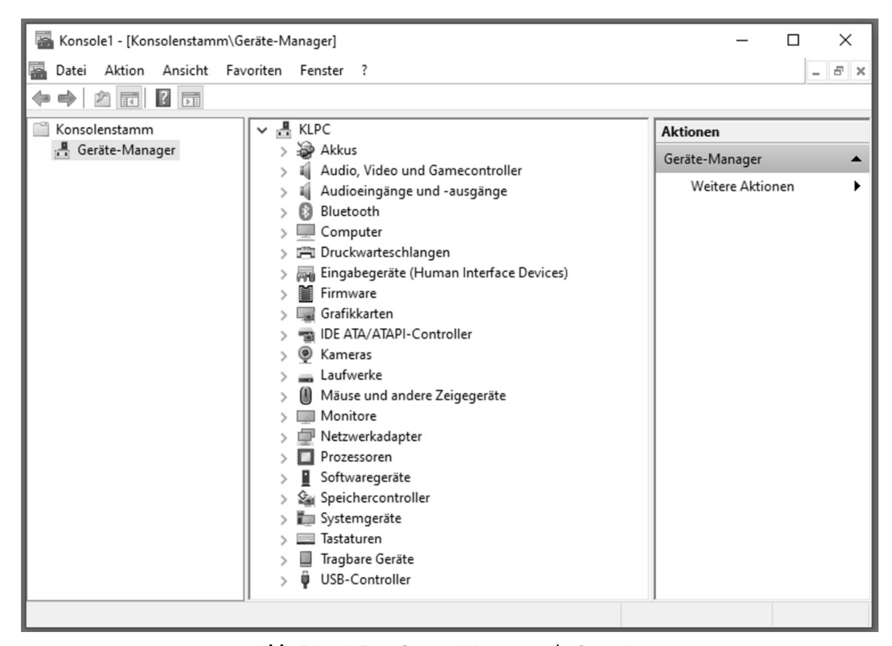


Abb. 14.26: Der Geräte-Manager als Snap-In

Nachdem Sie die erwünschten Snap-Ins hinzugefügt haben, können Sie die Konsole unter einem beliebigen Namen an einem beliebigen Ort speichern. Ich werde diese Konsole unter dem Namen GERÄTE-MANAGER speichern und eine Verknüpfung auf meinem Desktop ablegen (Abbildung 14.27). Jetzt brauche ich nur noch einen Doppelklick, um den Geräte-Manager zu öffnen.



Abb. 14.27: Verknüpfung mit dem Geräte-Manager auf dem Desktop

14.2 Betriebssysteme optimieren

Bei der Wartung versucht man zu verhindern, dass sich die Leistung eines Betriebssystems mit der Zeit verschlechtert. Aber natürlich ist Stillstand unerwünscht und unsere Systeme sollen besser, leistungsfähiger und schneller werden! Alles, was Sie tun, um Windows besser als zuvor zu machen, wie beispielsweise die Installation von Software oder Hardware, damit irgendetwas besser funktioniert, wird *Optimierung* genannt.

14.2.1 Software installieren und entfernen

Die häufigste Optimierung, die auf PCs vorgenommen wird, ist wahrscheinlich das Hinzufügen und Entfernen von Programmen. Die Installation und das Entfernen von Software gehören bei jedem PC zum Alltag. Immer wenn Sie Software hinzufügen oder entfernen, nehmen Sie Änderungen vor und treffen Entscheidungen, die das System über die Arbeitsweise dieser Software hinaus beeinflussen kann. Sie sollten also wissen, wie Sie es richtig machen.

Software installieren

Bei der Installation von Software auf einem Betriebssystem müssen verschiedene Dinge beachtet werden. Was sind die Systemanforderungen? Ist auf der Festplatte des Computers, auf die Software installiert werden soll, ausreichend Platz vorhanden? Verfügt er über genug Arbeitsspeicher, damit das Programm vernünftig läuft? (Denken Sie an Kapitel 11 und an die Systeme zur Bearbeitung von Videos, bei denen der Arbeitsspeicher aufgerüstet werden musste, damit die Software flüssig arbeitet.) Ist die Betriebssystemversion auf dem Rechner mit den Systemanforderungen der Software kompatibel?

Die Verfahren zur Installation von Software haben sich im Laufe der Jahre verändert. Lange wurde ein Großteil der Software auf Wechseldatenträgern vertrieben, wie auf Floppy Disks (das war in meiner Jugend), oder auf optischen Medien, wie CD-ROM oder DVD-ROM. Heutzutage ist die meiste Software im Internet erhältlich. In diesem Fall ist ein Download erforderlich.

Das Benutzerkonto, unter dem die Software installiert werden soll, muss über Administrator- oder Root-Rechte verfügen. Die Installation könnte auch mit erhöhten Rechten ausgeführt werden, sofern das Administratorkennwort bekannt ist.

Und schließlich sind bei der Installation auch Sicherheitsaspekte zu berücksichtigen. Welchen Einfluss hat die fragliche Anwendung auf die Sicherheit des Systems insgesamt? Ergibt eine Internetrecherche irgendwelche Hinweise auf Sicherheitslücken der Software und deren Ausnutzung? Welche Auswirkungen hat die Anwendung auf den Computer? Wird er anfälliger für Angriffe? Und wenn der Computer mit einem lokalen Netzwerk verbunden ist, welchen Einfluss könnte die Installation der Software auf das Netzwerk haben?

Das sind viele Fragen, die zu beantworten sind, auch wenn man nur eine einfache Anwendung installieren möchte, um Arbeit zu erledigen oder ein Spiel zu spielen. Die Beantwortung dieser Fragen kann dafür verantwortlich sein, ob Sie ein funktionierendes Netzwerk und flott arbeitende Computer oder einen richtig schlechten Tag vor sich haben. Beachten Sie diese Fragen, wenn Sie Software installieren.

Software unter Windows installieren

Sind Anwendungsprogramme nicht im Internet zum Herunterladen verfügbar, werden sie meist auf optischen Discs ausgeliefert. Windows unterstützt die Funktion *Autorun*, die gleich nach dem Einlegen bzw. Anschließen eines Datenträgers oder Speichermediums (optische Discs oder USB-Speichersticks) eine spezielle Datei namens `autorun.inf` liest und das darin genannte Programm automatisch startet. Die meisten auf Wechselmedien ausgelieferten Anwendungsprogramme verfügen über eine `autorun`-Datei, die das betreffende Installationsprogramm aufruft (Abbildung 14.28). Ganz ähnlich funktioniert *AutoPlay*. Dabei erscheint ein kleines Dialogfeld, wenn Sie den Wechseldatenträger ins Laufwerk einlegen. Die im Dialogfeld angebotenen Optionen hängen davon ab, was Windows auf dem Laufwerk vorfindet. Dazu könnte auch eine Autorun-Anwendung gehören.

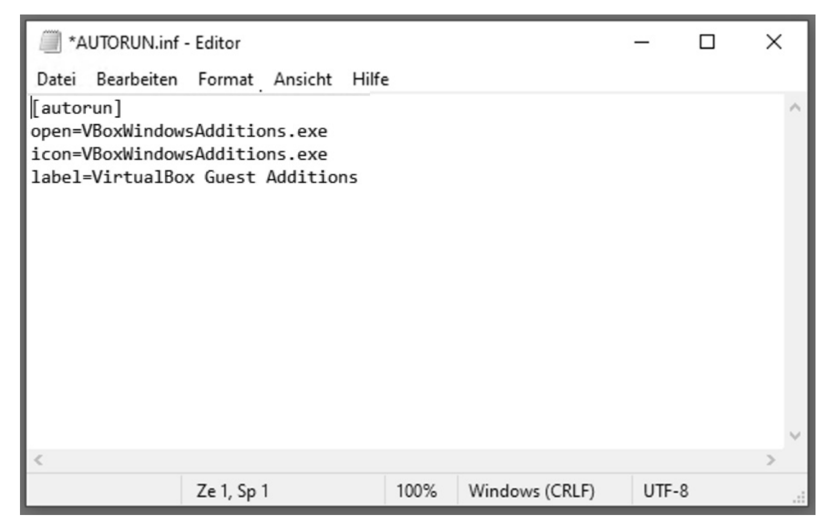


Abb. 14.28: Eine `AUTORUN.inf`-Datei im Editor

Manchmal müssen Sie Programme aber auch manuell installieren. Doppelklicken Sie dazu im Explorer auf das Symbol der Disc. Alle Betriebssysteme suchen anschließend ausführbare Programme auf der Disc oder dem Wechseldatenträger an, die Sie dann starten.

Unter Windows erschwert die Benutzerkontensteuerung (UAC) den Installationsprozess ein wenig. Wahrscheinlich wird bei der Installation einer Anwendung eine Meldung der Benutzerkontensteuerung angezeigt. Dann haben Sie ein wenig Zeit, um zu registrieren, was mit Ihrem System geschieht, und können die Installation des Programms unterbinden. Wenn Sie ein Administratorkonto verwenden, dann können Sie einfach JA oder FORTSETZEN anklicken und die Installation abschließen (Abbildung 14.29).



Abb. 14.29: Die Benutzerkontensteuerung bei einer Installation

Wenn Sie sich über ein Konto mit weniger Rechten angemeldet haben, dann müssen Sie den Namen und das Kennwort eines Kontos mit Administratorberechtigungen eingeben. Einige Installationsprogramme informieren die Benutzerkontensteuerung nicht richtig darüber, dass mehr Berechtigungen benötigt werden, und versagen einfach – und zwar unabhängig von den Berechtigungen des Kontos, über das Sie sich angemeldet haben. In derartigen Fällen klicken Sie das Symbol des Installationsprogramms besser mit der rechten Maustaste an und wählen im Kontextmenü ALS ADMINISTRATOR AUSFÜHREN, um dem Programm gleich zu Beginn die von ihm erwarteten Rechte einzuräumen.

Wenn alle Voraussetzungen erfüllt sind, müssen Sie normalerweise vor der Installation der Anwendung den Bestimmungen der Softwarelizenz zustimmen. Dieser Schritt ist verbindlich, da die Installation nicht fortgesetzt werden kann, wenn Sie nicht alle Bestimmungen des Softwareherstellers akzeptiert haben (Abbildung 14.30). Unter Umständen müssen Sie während des Installationsprozesses noch verschiedene weitere Entscheidungen treffen. Beispielsweise werden Sie danach gefragt, wo das Programm installiert werden soll und ob Sie die Installation zusätzlicher Programmkomponenten wünschen. Sofern keine wichtigen Gründe dagegen sprechen, ist es generell immer am einfachsten, die empfohlenen Einstellungen zu übernehmen.

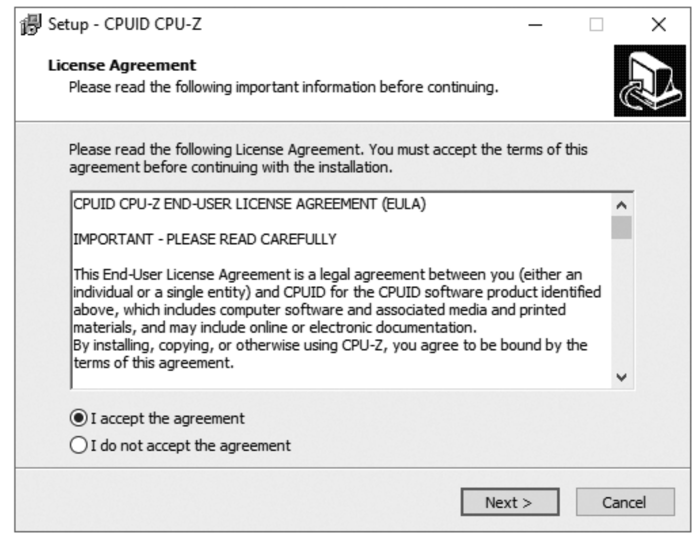


Abb. 14.30: Akzeptieren der Lizenzbedingungen

Zu Windows 10 gehört immer auch der Microsoft Store. Microsoft prüft die dort angebotenen Anwendungen, um zu gewährleisten, dass sie sicher sind und keine Schadsoftware enthalten (Abbildung 14.31). Über den Microsoft Store wird nur ein geringer Prozentsatz aller Anwendungen installiert. Die meisten Leute ziehen es vor, die herkömmlichen Verfahren zur Installation von Software zu verwenden.

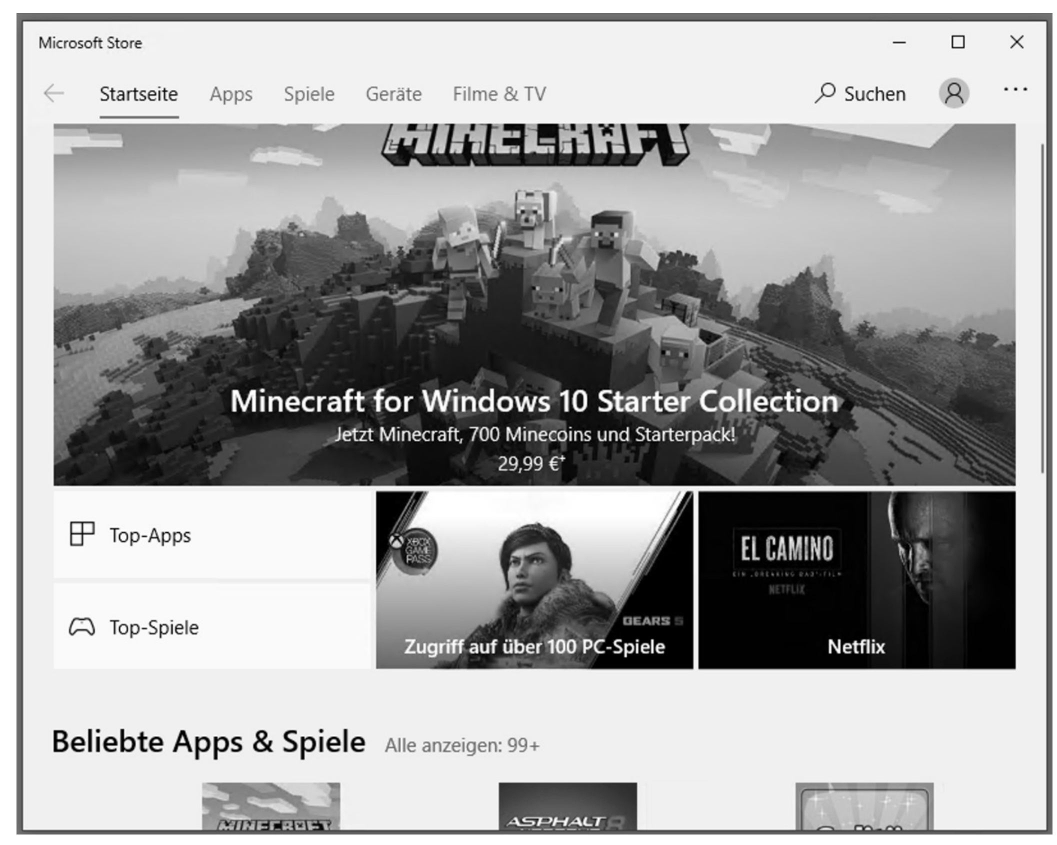


Abb. 14.31: Microsoft Store

Software installieren in macOS

macOS bietet mehrere Möglichkeiten zur Installation von Software. Eine der gebräuchlichsten Methoden ist die Verwendung des Mac App Stores, der über das Apple-Menü erreichbar ist (Abbildung 14.32). Der Installationsvorgang hat große Ähnlichkeit mit dem Installieren einer App auf einem Smartphone. Sie klicken auf LADEN oder APP KAUFEN und geben Ihre Anmeldedaten ein. Dann klicken Sie auf INSTALLIEREN und die App wird installiert.

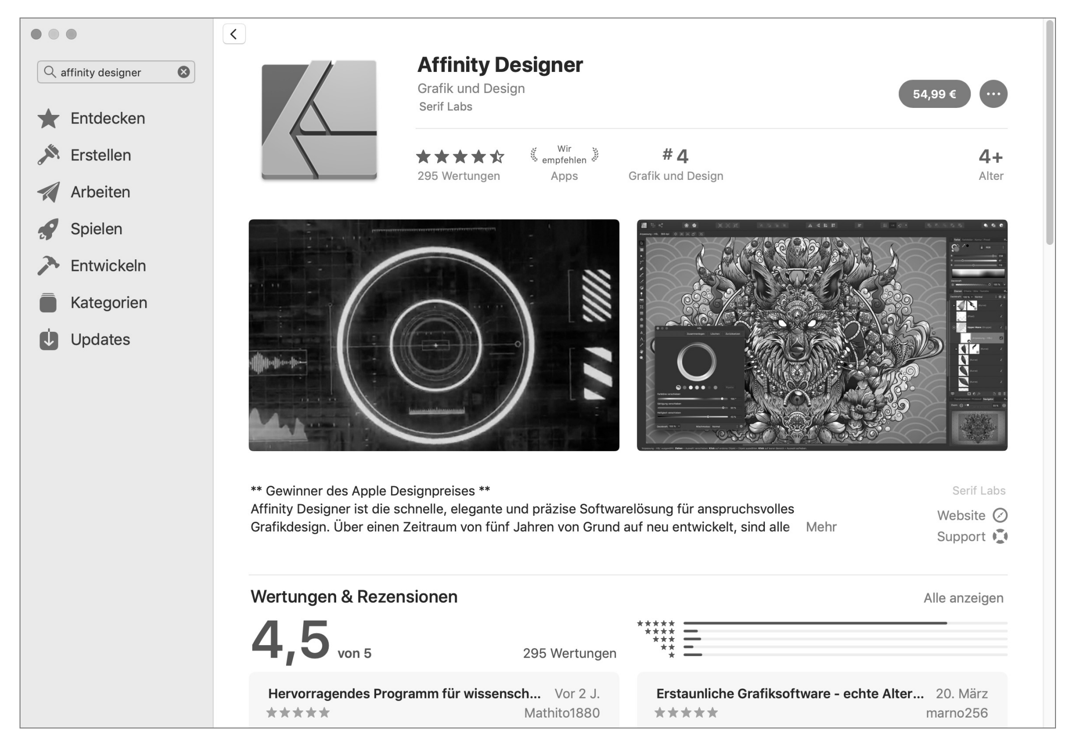


Abb. 14.32: Das Programm AFFINITY DESIGNER im Mac App Store

Alternativ können Sie auch Installationsprogramme herunterladen, die oft als `.dmg`-Dateien bereitgestellt werden. Nach dem Öffnen kopieren Sie dann die auf dem Image enthaltene Software einfach per Drag-and-Drop in den Ordner PROGRAMME oder starten ein auf dem Image befindliches Installationsprogramm, das Sie durch die Programminstallation führt.

Software installieren unter Linux

Die Installationsvorgänge der verschiedenen Linux-Distributionen unterscheiden sich ein wenig voneinander. Viele Distributionen, wie etwa Ubuntu, bieten einen Store, der ähnlich wie der Microsoft Store oder der Mac App Store funktioniert (Abbildung 14.33). Eine weitere Möglichkeit ist, ein Installationsprogramm herunterzuladen, das Sie per Doppelklick starten. Dann wählen Sie unter den verfügbaren Optionen INSTALLIEREN aus.

Die häufigste Methode, neue Anwendungen zu installieren, ist der Einsatz einer Paketverwaltung, wie das *Advanced Package Tool* (APT) von Ubuntu. Sie können es im Terminal mit den Befehlen `apt-get` oder `apt` verwenden. (Mehr über Befehle imTerminal erfahren Sie in Kapitel 15.) Interessanterweise verwendet die grafische Benutzeroberfläche für den Ubuntu-Store hinter den Kulissen tatsächlich `apt`.

Wichtig

Windows, macOS und Linux verlangen bei einer Installation die Eingabe der Anmeldedaten eines Benutzers mit Administrator- oder `root`-Rechten. Manchmal müssen Sie daher Ihr Kennwort mehrmals eingeben, bevor der Installationsvorgang abgeschlossen werden kann.

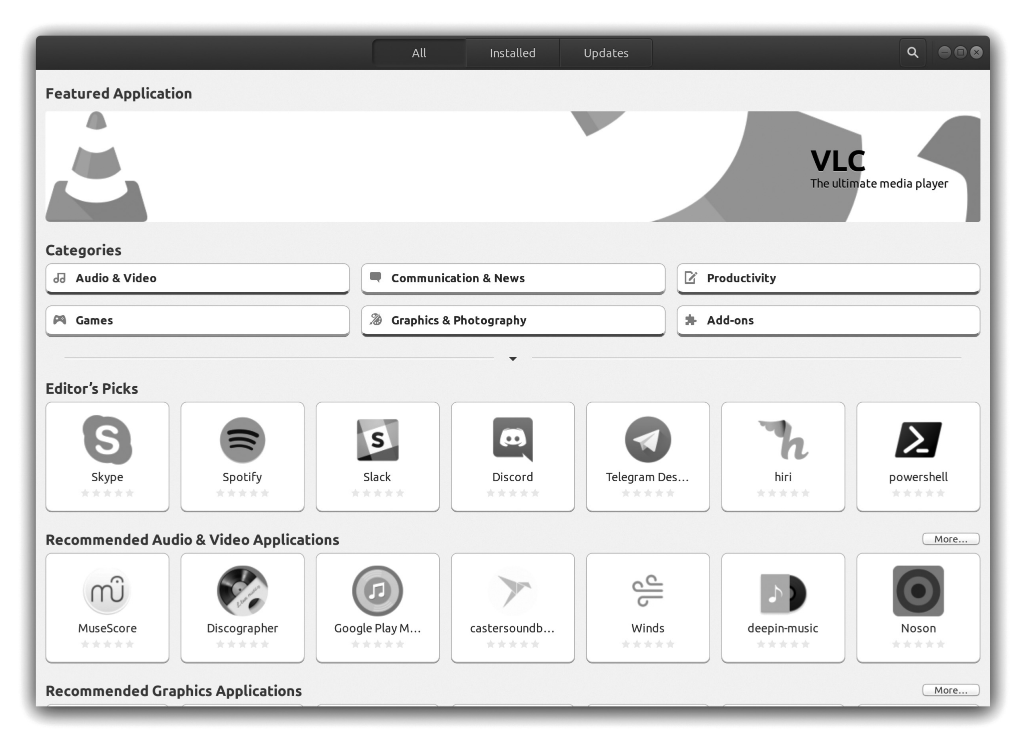


Abb. 14.33: Optionen im Linux Store

Software entfernen

Jede installierte Anwendung benötigt Platz auf der Festplatte. Nicht länger benötigte Programme verschwenden also Platz, der für andere Zwecke sinnvoller verwendet werden könnte. Das Entfernen dieser Programme gehört daher zu den wichtigen Aufgaben im Rahmen der Optimierung.

Das Entfernen eines Programms von einem Windows-PC läuft ähnlich wie die Installation ab. Dazu sollten Sie möglichst das Deinstallationsprogramm der Anwendung verwenden. Sie finden es in der Regel in der Programmgruppe der betreffenden Anwendung im Startmenü (Abbildung 14.34).

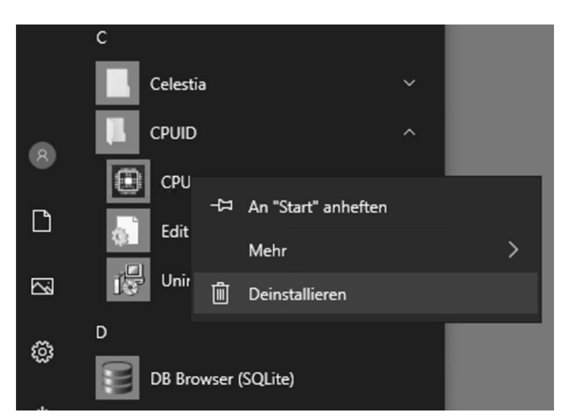


Abb. 14.34: Deinstallieren eines Programms

Falls kein Deinstallationsprogramm zur Verfügung stehen sollte, verwenden Sie das Applet PROGRAMME UND FEATURES in der Systemsteuerung oder APPS & FEATURES in der Einstellungs-App. Abbildung 14.35 zeigt dieses Applet unter Windows 10. Sie doppelklicken auf das zu entfernende Programm aus und klicken anschließend die Schaltfläche DEINSTALLIEREN an. Sie brauchen keine Sorge zu haben: Die Anwendung wird nun nicht auf einmal gelöscht. Als Erstes erhalten Sie eine Meldung angezeigt, die Sie darauf hinweist, dass das Programm nun dauerhaft von Ihrem PC entfernt wird. Wenn es das ist, was Sie möchten, klicken Sie auf JA.

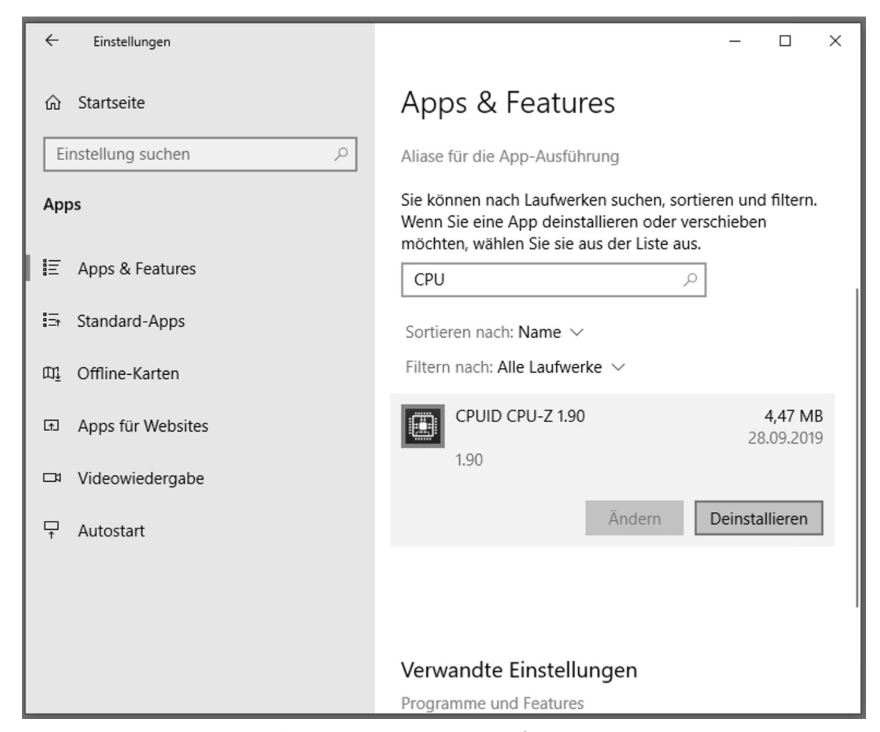


Abb. 14.35: Das Applet APPS & FEATURES

Unter Umständen erscheint dann noch eine Meldung, die Sie darauf hinweist, dass eine gemeinsam genutzte Datei, die anscheinend nicht länger benötigt wird, nun gelöscht werden wird. Diesen Vorgang müssen Sie dann bestätigen (bzw. ablehnen). Generell ist es besser, solche Dateien zu löschen. Falls Sie diese nicht löschen, werden sie sehr wahrscheinlich als nutzlose Dateien auf Ihrem Computer herumliegen und nichts anderes tun, als ewig Platz zu belegen. In manchen Fällen wird durch das Anklicken der Schaltfläche ÄNDERN/ENTFERNEN das Deinstallationsprogramm der Anwendung gestartet (das Programm, das Sie zuvor nicht finden konnten). Sie können dann die installierten Programmfunktionen ändern. Diese Funktion gehört nicht zu Windows, sondern zu dem zu entfernenden Programm. Zum Schluss der Aktion sollten dann die einzelnen Bestandteile und Registry-Einträge der Anwendung vom Rechner gelöscht werden.

Hinweis

On die Schaltfläche ÄNDERN/ENTFERNEN oder DEINSTALLIEREN angezeigt wird, hängt vom jeweiligen Programm ab. Nicht alle Anwendungen können geändert werden.

In macOS hängt das Deinstallieren davon ab, wie ein Programm installiert wurde. Aus dem Mac App Store heruntergeladene Programme werden ähnlich wie auf einem Smartphone deinstalliert. Zunächst einmal öffnen Sie über das Dock oder im Ordner PROGRAMME die App LAUNCHPAD (das Programmsymbol stellt eine Rakete dar). Klicken Sie dann auf irgendeine App und halten Sie die Maustaste gedrückt, bis alle Programmsymbole anfangen zu »zappeln« (oder drücken Sie die `Alt`-Taste). Neben Programmen, die sich deinstallieren lassen, erscheint dann oben links ein X in einem Kreis (Abbildung 14.36. Klicken Sie darauf, um die App zu entfernen. Falls Sie ein Programm versehentlich gelöscht haben, können Sie es erneut im Mac App Store herunterladen.



Abb. 14.36: Deinstallieren von Apps aus dem Mac App Store mit der App LAUNCHPAD

Für alle anderen Apps gibt es in macOS zwei Methoden zum Deinstallieren. Ziehen Sie das Programm einfach in den Papierkorb oder verwenden Sie das Deinstallationsprogramm, falls es ein solches gibt. Die erste Methode, nämlich ein Programm einfach zu löschen, ist am gebräuchlichsten, denn eigene Deinstallationsprogramme gibt es nur für größere, oft auch plattformübergreifende Programmpakete wie z.B. Photoshop. Sie sollten aber wissen, dass beim Löschen eines Programms oft einige Dateien im System verbleiben, hauptsächlich in Form von Benutzereinstellungen im LIBRARY-Ordner des Benutzers.

Das Entfernen von Programmen in den gängigen Linux-Distributionen ist genauso einfach wie das Installieren. Öffnen Sie das Programm zum Verwalten von Software, wählen Sie die App aus und klicken Sie auf ENTFERNEN (Abbildung 14.37). Die Paketverwaltung, mit der wir uns in Kapitel 15, *Eingabeaufforderung*, noch eingehend befassen werden, übernimmt die eigentliche Arbeit für Sie und entfernt die Dateien.



Abb. 14.37: Entfernen einer Anwendung in Ubuntu

Windows-Komponenten hinzufügen und entfernen

Während der Installation versucht Windows festzustellen, welche der optionalen Windows-Komponenten Sie benötigen. So werden beispielsweise der Editor, die Netzwerkunterstützung oder Spiele auf Ihrem PC installiert. Sie können Windows-Komponenten dieser Art jederzeit von Ihrem System entfernen oder auch weitere Komponenten nach Wunsch hinzufügen.

Starten Sie in der Systemsteuerung das Applet PROGRAMME UND FEATURES und wählen Sie dann in der Aufgabenliste WINDOWS-FEATURES AKTIVIEREN ODER DEAKTIVIEREN. Bestätigen Sie gegebenenfalls die Abfrage der Benutzerkontensteuerung. Nun wird das Dialogfeld für Windows-Features geöffnet (Abbildung 14.38). Klicken Sie einfach auf die Kontrollkästchen, um Features zu aktivieren oder zu deaktivieren.

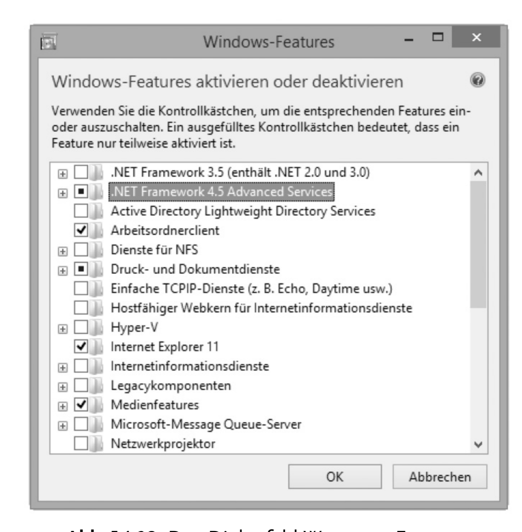


Abb. 14.38: Das Dialogfeld WINDOWS-FEATURES

14.2.2 Installieren und Optimieren von Geräten

Die Installation neuer Hardware erfolgt unter den verschiedenen Windows-Versionen auf dieselbe Weise und die Schritte zur Problembehebung ähneln denen bei der Installation neuer Geräte stark. Der Installationsprozess wird in den jeweiligen Kapiteln dieses Buchs genauer beschrieben, in denen es um die verschiedenen Gerätetypen geht. Rufen Sie sich auch die Optimierungen und Fehlerbehebungen ins Gedächtnis, über die Sie in Kapitel 6, *Mainboards*, gelesen haben oder schlagen Sie dort nach, wenn eine der nachfolgend beschriebenen Aktionen Ihnen unklar erscheint.

Hier sind die Schritte, die es zu beachten gilt:

- Aktualisieren Sie die Treiber (die für gewöhnlich von der Website des Herstellers stammen).
- Überprüfen Sie, ob das Gerät ordnungsgemäß funktioniert.
- Kehren Sie zu den vorherigen Treibern zurück, falls sich der neue Treiber als fehlerhaft erweisen sollte.
- Verwenden Sie keine Betaversionen von Treibern.

Treiberaktualisierung in macOS

macOS benachrichtigt Sie, wenn Systemaktualisierungen verfügbar sind, die Treiber für die eingebauten Komponenten beinhalten. Öffnen Sie die Systemeinstellungen und klicken Sie auf SOFTWAREUPDATES, um zu überprüfen, ob Aktualisierungen vorliegen (Abbildung 14.39). Wenn Sie Geräte von Drittherstellern einsetzen, wie z.B. ein Wacom-Tablett, müssen Sie gegebenenfalls selbst nach neuen Treibern suchen und diese aktualisieren.

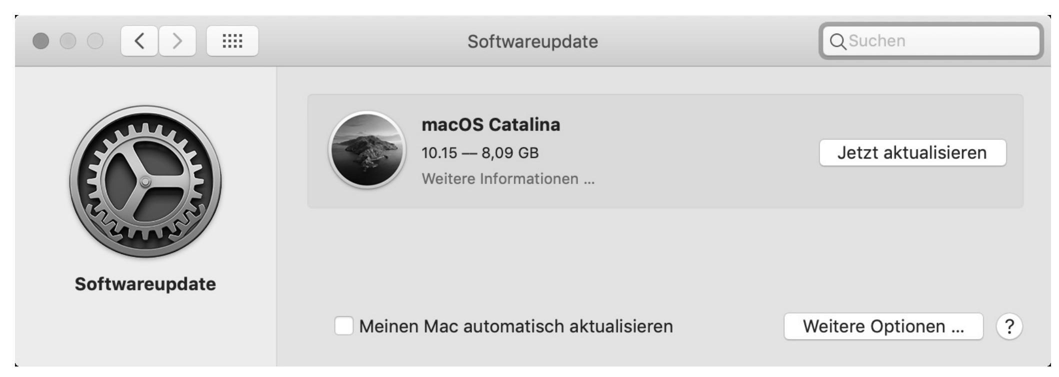


Abb. 14.39: Für diesen Mac steht eine neue Betriebssystemversion zur Verfügung.

Hinweis

Im Gegensatz zu Windows Update können Softwareupdates für macOS auch Treiber und Firmware von Apple-Computern aktualisieren. Schließlich ist Apple letzten Endes ein Hardware-Hersteller.

Treiberaktualisierung in Linux

Die meisten Linux-Distributionen suchen regelmäßig automatisch nach Updates und benachrichtigen Sie, wenn es welche gibt. Zum Herunterladen und Installieren der Updates gibt es ein Werkzeug zur Verwaltung von Software.

Geräte-Manager

Als es um die Installation und die Fehlersuche für Geräte ging, haben Sie in anderen Kapiteln bereits mit dem Geräte-Manager gearbeitet. Aber auch für die Optimierung von Gerätetreibern brauchen Sie

ihn. Klicken Sie im Geräte-Manager ein Gerät mit der rechten Maustaste an, um das Kontextmenü anzeigen zu lassen. Von hier aus können Sie den Treiber aktualisieren oder deinstallieren, das Gerät deaktivieren, nach Hardwareänderungen suchen oder das Dialogfeld EIGENSCHAFTEN anzeigen lassen. Dort finden Sie abhängig vom jeweiligen Gerät mehrere Registerkarten. Bei den meisten Geräten gibt es die Registerkarten ALLGEMEIN, TREIBER, DETAILS und RESSOURCEN. Für die Optimierung ist die Registerkarte TREIBER am wichtigsten.

Auf der Registerkarte TREIBER finden Sie die Schaltflächen TREIBERDETAILS, TREIBER AKTUALISIEREN, VORHERIGER TREIBER, GERÄT DEAKTIVIEREN und GERÄT DEINSTALLIEREN. Die meisten davon kennen Sie schon aus Kapitel 6. Mit TREIBERDETAILS können Sie die Treiberdateien und deren Speicherorte auf der Festplatte anzeigen.

Ein neues Gerät hinzufügen

Windows sollte automatisch neue Geräte erkennen, die dem System hinzugefügt werden. Gelingt die Erkennung nicht, können Sie die Option GERÄT HINZUFÜGEN im Applet GERÄTE UND DRUCKER verwenden (Abbildung 14.40), um das Gerät zu erkennen und den Treiber zu installieren.

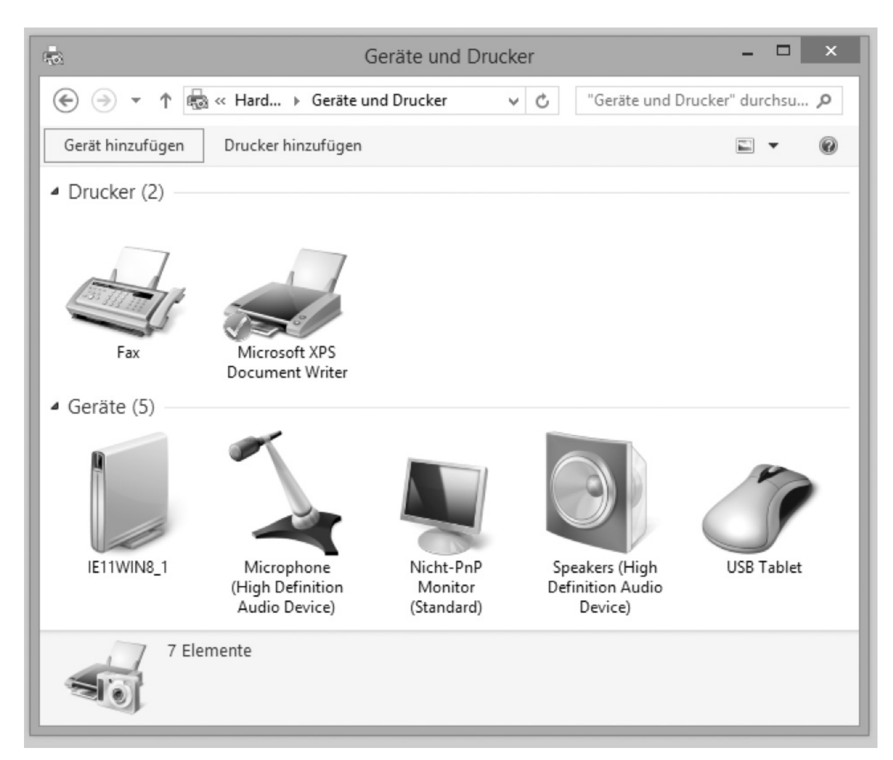


Abb. 14.40: Hinzufügen neuer Geräte in Windows 8.1

14.2.3 Leistungsoptionen

Über LEISTUNGSOPTIONEN können Sie unter allen Windows-Versionen Optimierungen vornehmen. Hier können Sie die Einstellungen für CPU, RAM und virtuellen Speicher (Auslagerungsdatei) konfigurieren. Um auf diese Optionen zuzugreifen, klicken Sie COMPUTER oder DIESER PC mit der rechten Maustaste an, wählen im Kontextmenü EIGENSCHAFTEN und klicken dann in der Aufgabenliste die Option ERWEITERTE SYSTEMEINSTELLUNGEN an. Wählen Sie dort im Bereich LEISTUNG dann EINSTELLUNGEN aus.

Das Dialogfeld LEISTUNGSOPTIONEN enthält drei Registerkarten: VISUELLE EFFEKTE, ERWEITERT und DATENAUSFÜHRUNGSVERHINDERUNG (Abbildung 14.41). Auf der Registerkarte VISUELLE EFFEKTE können Sie die visuellen Effekte anpassen, die sich auf die Leistung auswirken könnten, wie z.B. Animationen, Miniaturansichten oder Transparenzen. Klicken Sie die oberen drei Auswahlmöglichkeiten an und beobachten Sie die Liste mit den Einstellungen. Beachten Sie die kleinen Unterschiede zwischen den beiden ersten Auswahlmöglichkeiten. Die dritte Auswahlmöglichkeit, FÜR OPTIMALE LEISTUNG ANPASSEN, deaktiviert alle visuellen Effekte, und die vierte Option (BENUTZERDEFINIERT) ist eine Einladung, eigene Anpassungen vorzunehmen.

Wenn Sie einen Computer benutzen, dessen Leistung für Windows so gerade eben ausreicht, kann die Deaktivierung der visuellen Effekte gewaltige Unterschiede bei der »gefühlten« Geschwindigkeit bedeuten. Meist können Sie die Einstellungen aber unverändert lassen.

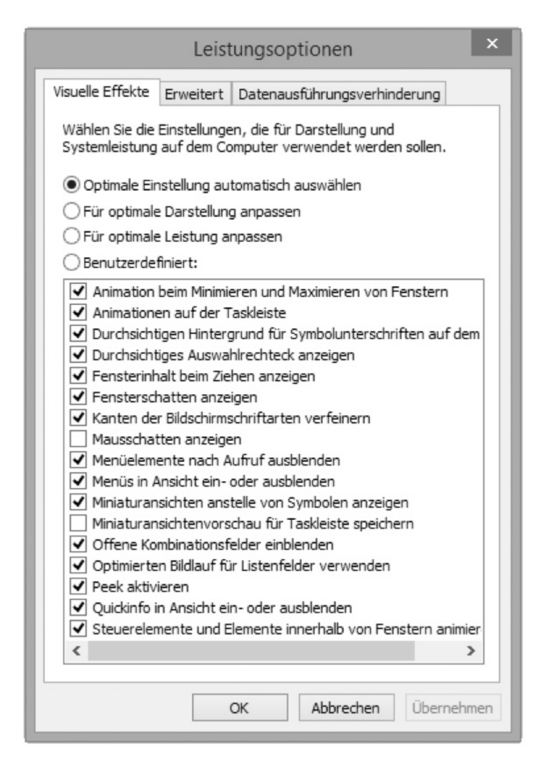


Abb. 14.41: Das Dialogfeld LEISTUNGSOPTIONEN in Windows 8.1

Auf der Registerkarte ERWEITERT (Abbildung 14.42) gibt es zwei Bereiche: PROZESSORZEITPLANUNG und VIRTUELLER ARBEITSSPEICHER. Im Bereich PROZESSORZEITPLANUNG können Sie die beste Leistung für Programme oder für Hintergrunddienste festlegen. Über den Bereich VIRTUELLER ARBEITSSPEICHER können Sie die Größe und die Speicherposition der Auslagerungsdatei ändern.

Die *Datenausführungsverhinderung* (*DEP*, *Data Execution Prevention*) läuft im Hintergrund und verhindert, dass Viren oder andere Malware die Kontrolle über Programme im Systemspeicher übernehmen. Sie verhindert nicht, dass Viren auf Ihrem Computer installiert werden, kann deren Wirkung aber abschwächen. Standardmäßig überwacht die Datenausführungsverhinderung nur kritische Betriebssystemdateien im RAM, aber über die Registerkarte DATENAUSFÜHRUNGSVERHINDERUNG können Sie auch dafür sorgen, dass alle ausgeführten Programme überwacht werden. Das funktioniert, bremst aber womöglich das System aus. Vielleicht stellen Sie auch fest, dass manche Programme abstürzen, wenn die Datenausführungsverhinderung für alle Programme aktiviert ist. Wie bei den anderen Optio-

nen im Dialogfeld LEISTUNGSOPTIONEN ist es auch hier meist am sinnvollsten, die Einstellungen unverändert zu lassen.

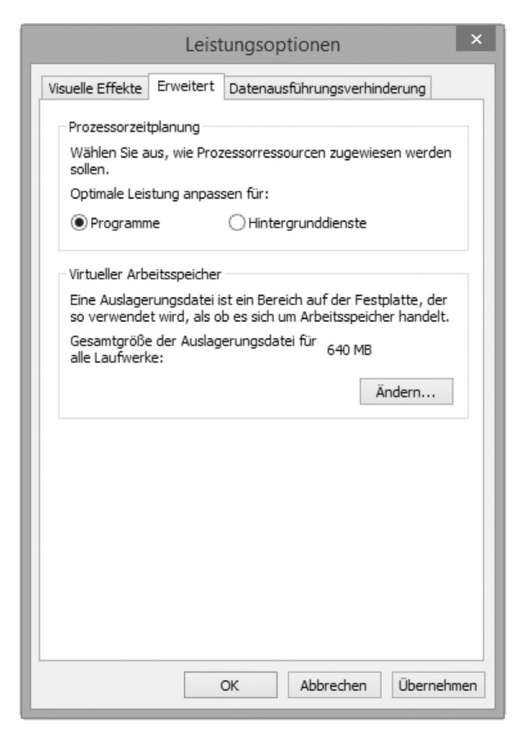


Abb. 14.42: Registerkarte ERWEITERT des Dialogfelds LEISTUNGSOPTIONEN

14.3 Auf Probleme vorbereitet sein

Im Rahmen der Optimierung von Windows müssen Techniker Vorbereitungen für den Fall von Problemen treffen. Alle modernen Betriebssysteme bieten die Möglichkeit einer Datensicherung, und wie Sie sich sicher vorstellen können, verfügen alle über andere Features. Auch Windows bietet die Möglichkeit einer Systemwiederherstellung. Sehen wir uns die vorbeugenden Maßnahmen, die man ergreifen kann, etwas genauer an.

14.3.1 Sicherung persönlicher Daten

Bei den wichtigsten Daten auf Ihrem Rechner handelt es sich um Ihre persönlichen Daten: Ihre Dokumente, E-Mail-Nachrichten und Kontakte, Internetfavoriten, Fotos und andere Dateien. Zur Sicherung persönlicher Daten gehört bei allen Windows-Versionen irgendein Sicherungsprogramm zum Lieferumfang. Und natürlich gibt es für macOS und Linux ebenfalls derartige Software.

Das Applet Sichern und Wiederherstellen unter Windows 7

Microsoft liefert mit Windows Windows 7 das Applet SICHERN UND WIEDERHERSTELLEN aus, ein einfaches automatisiertes Datensicherungsprogramm. Sie werden zunächst aufgefordert, einen Speicherort für die Sicherung anzugeben (Abbildung 14.43).

Anschließen fragt Windows, welche Daten Sie sichern möchten (Abbildung 14.44). Es gibt zwei Möglichkeiten: AUSWAHL DURCH WINDOWS (EMPFOHLEN) und AUSWAHL DURCH BENUTZER.

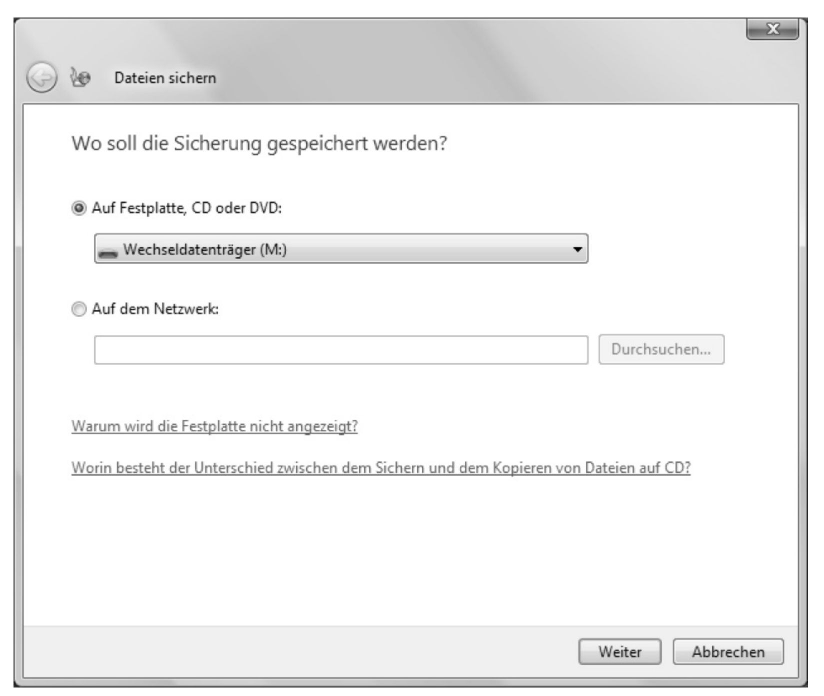


Abb. 14.43: Auswahl des Speicherorts

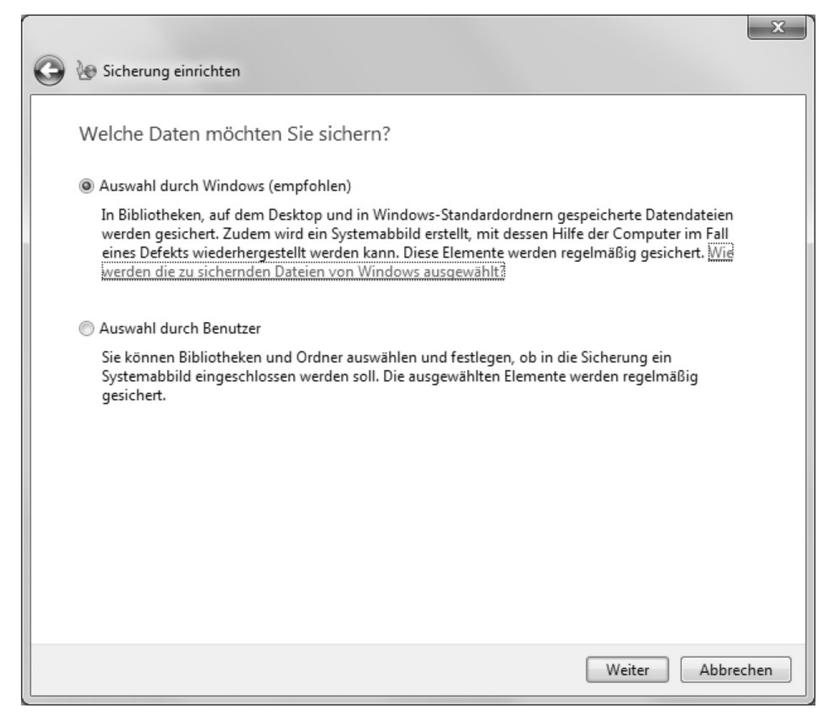


Abb. 14.44: Auswahl der zu sichernden Daten

Wichtig

Inhalte, die sich nicht auf NTFS-Laufwerken befinden, können mit Windows nicht gesichert werden.

Wenn Sie AUSWAHL DURCH WINDOWS (EMPFOHLEN) auswählen, wird eine Sicherung ähnlich der in Windows Vista erstellt, jedoch mit einem wichtigen Unterschied. Neben den persönlichen Benutzerdaten wird außerdem (vorausgesetzt, es ist genügend Speicherplatz vorhanden) automatisch ein Systemabbild erstellt, das nicht nur das vollständige Betriebssystem enthält, sondern darüber hinaus alle installierten Programme, Gerätetreiber und sogar die Registry.

Der Punkt AUSWAHL DURCH BENUTZER ist ebenfalls interessant. Windows 7 erlaubt es, einzelne Benutzer auszuwählen (Abbildung 14.45). Das erweist sich als praktisch, wenn Sie Daten sichern möchten, die sich außerhalb der Ordner befinden, die AUSWAHL DURCH WINDOWS umfasst.

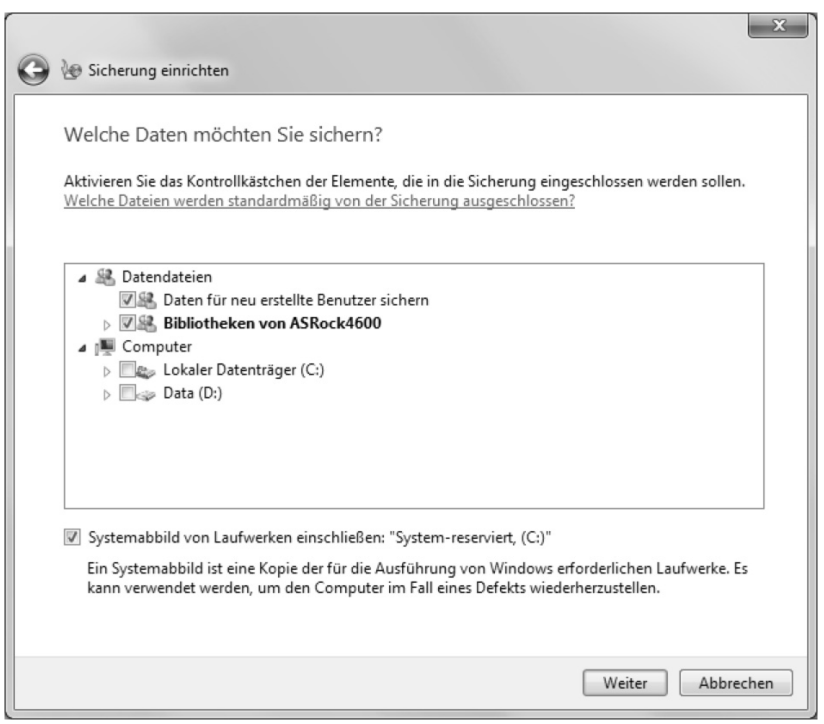


Abb. 14.45: Auswahl der zu sichernden Elemente

Nach Anwahl eines Benutzers können Sie, wie in Abbildung 14.46, einzelne Bibliotheken und Ordner des Benutzers aktivieren oder deaktivieren. Beachten Sie außerdem das Kontrollkästchen, das es Ihnen erlaubt, ein Systemabbild zu erstellen, ganz als ob Sie die Option AUSWAHL DURCH WINDOWS (EMPFOHLEN) gewählt hätten.

Nach Abschluss der Einstellungen nimmt der Assistent seine Arbeit auf und Windows führt die Sicherung durch. Während die Sicherung läuft, können Sie den Vorgang anhand einer praktischen und hochspannenden Fortschrittsanzeige beobachten (Abbildung 14.47). Wenn Ihnen das zu aufregend ist, können Sie das Sicherungsfenster einstweilen auch schließen. Bei einer großen Festplatte kann der Vorgang ein Weilchen dauern (bis zu einigen Stunden).

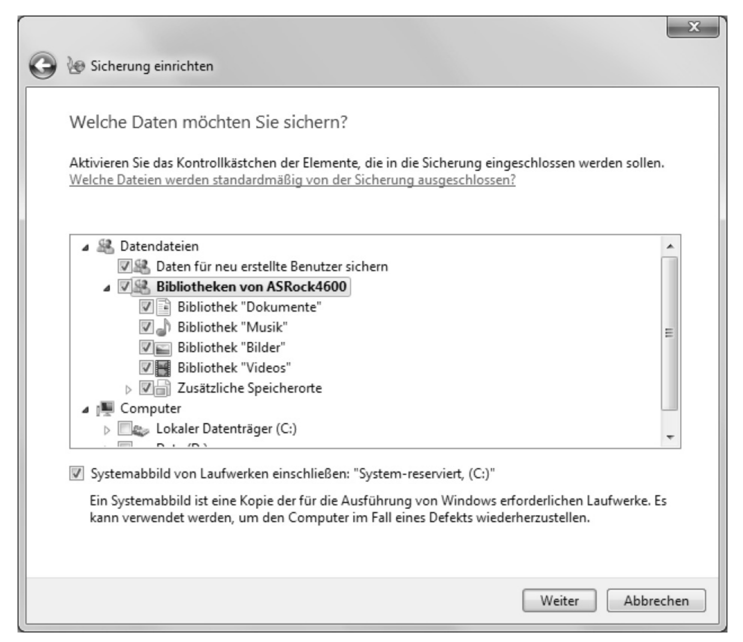


Abb. 14.46: Die Bibliotheken und Ordner eines einzelnen Benutzers

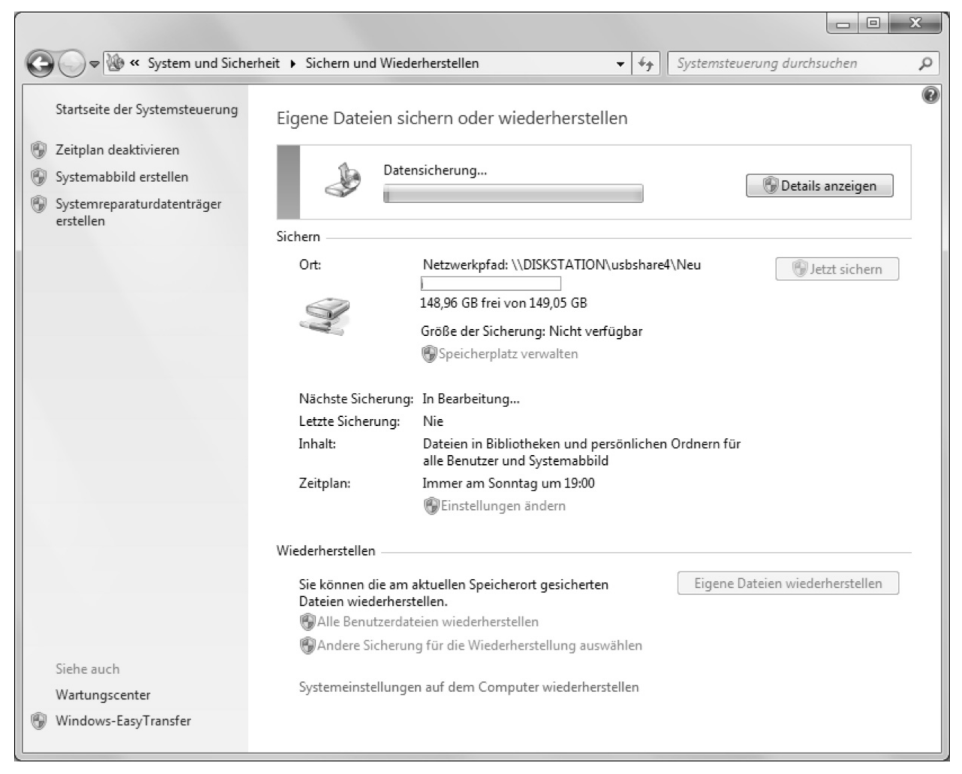


Abb. 14.47: Die Datensicherung läuft ...

Hinweis

In Windows 7 können Sie auch ausschließlich ein Systemabbild erstellen. Wählen Sie im Applet SICHERN UND WIEDERHERSTELLEN einfach SYSTEMABBILD ERSTELLEN aus.

Dateiversionsverlauf in Windows 8/8.1/10

Mit Windows 8 hat Microsoft in der Systemsteuerung das Applet DATEIVERSIONSVERLAUF eingeführt, das es ermöglicht, die persönlichen Dateien und Ordner eines Benutzers zu sichern (Abbildung 14.48). Der Dateiversionsverlauf erfordert ein weiteres Laufwerk und ist daher standardmäßig deaktiviert. Sie können als weiteres Laufwerk eine beliebige interne oder externe Festplatte oder SSD verwenden. (Sie könnten vermutlich auch eine andere Partition auf demselben Laufwerk verwenden, aber das ergibt ja eigentlich keinen Sinn.) Aktivieren Sie den Dateiversionsverlauf, um Ihre Bibliotheken, Ihren Desktop, Ihre Kontakte und Favoriten zu sichern.

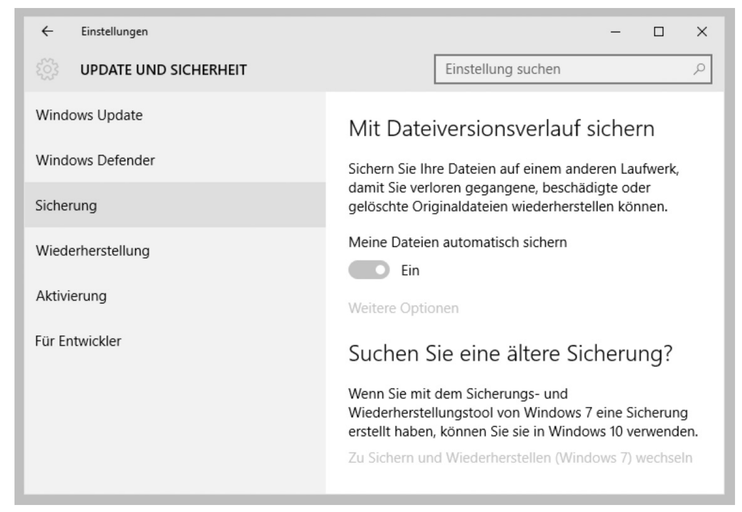


Abb. 14.48: Dateiversionsverlauf in Windows 10

Beachten Sie, dass der Dateiversionsverlauf Ihre persönlichen Daten nur dann sichert, wenn Sie die Daten entweder zu den Standardbibliotheken hinzufügen oder benutzerdefinierte Bibliotheken erstellt haben. Der Dateiversionsverlauf ist keinesfalls ein Ersatz für eine vollständige Datensicherung des Systems. Microsoft empfiehlt, Software von Drittherstellern zu verwenden, um ein vollständiges Backup des Systems unter Windows 8 oder neuer zu erstellen.

Hinweis

In Windows 8/8.1 gab es außer dem Dateiversionsverlauf kein Programm zur Datensicherung. In Windows 10 kehrte das Datensicherungsprogramm von Windows 7 zurück, das im Dateiversionslauf sogar als SICHERN UND WIEDERHERSTELLEN (WINDOWS 7) bezeichnet wird.

Time Machine in macOS

macOS stellt mit dem ausgezeichneten Programm *Time Machine* eine Lösung zum Erstellen von vollständigen Backups bereit (Abbildung 14.49). Bei diesen Sicherungen handelt es sich um Momentaufnahmen des lokalen Systems. Mit Time Machine können Sie ausgewählte oder alle Dateien wiederherstellen, falls Ihre Festplatte ausfällt. Außerdem ist es möglich, gelöschte Dateien oder ältere Versionen von

Dateien wiederherzustellen. Time Machine benötigt eine zweite Festplatte oder SSD, kann aber auch ein Netzlaufwerk verwenden. Sie finden Time Machine in den Systemeinstellungen.



Abb. 14.49: Time Machine

Datensicherungen in Linux

Die verschiedenen Linux-Distributionen verwenden unterschiedliche Programme zur Sicherung von Dateien, Ordnern und Laufwerken. In Ubuntu kommt *Déjà Dup* zum Einsatz, erscheint in den Systemeinstellungen allerdings unter der Bezeichnung Datensicherungen (Abbildung 14.50). Déjà Dup speichert die Dateien so, wie Sie es angeben, also auf externen Festplatten, Netzwerklaufwerken oder sogar in einem Ordner auf der Hauptfestplatte (was natürlich nicht zu empfehlen ist, wenn Ihnen an Ihren Daten etwas liegt!). Déjà Dup sichert standardmäßig den Home-Ordner eines Benutzers, denn dort legen die meisten Benutzer ihre persönlichen Daten ab. Déjà Dup speichert alle Versionen der Dateien dauerhaft, sofern der verfügbare Speicherplatz dafür ausreicht.



Abb. 14.50: DATENSICHERUNGEN in den Systemeinstellungen von Ubuntu

14.3.2 Systemwiederherstellung in Windows

Jeder Techniker kann die eine oder andere Geschichte über Benutzer erzählen, die ihren PC mit der neuesten Hardware und der coolsten Software ausstatten wollten. Dann kam die große Überraschung und nichts ging mehr: Das System hängte sich auf, startete nicht mehr oder verhielt sich einfach nur noch höchst seltsam. Und natürlich konnte sich der Benutzer nicht mehr daran erinnern, was er wann installiert hatte. Dann weiß er nur noch, dass Sie das Problem möglichst schnell wieder beheben sollen – und zwar schleunigst!

Mit der *Systemwiederherstellung* können Sie *Wiederherstellungspunkte* definieren, bei denen es sich um Kopien der Computerkonfiguration zu einem bestimmten Zeitpunkt handelt. Bei einem späteren Absturz oder einem beschädigten Betriebssystem können Sie damit das System wieder in seinen früheren Zustand zurückversetzen.

Die Systemwiederherstellung ist weitgehend automatisiert und das Betriebssystem erstellt selbstständig eine Reihe von Wiederherstellungspunkten. Um einen eigenen Wiederherstellungspunkt zu erstellen, klicken Sie im Explorer mit der rechten Maustaste auf COMPUTER oder DIESER PC und wählen EIGENSCHAFTEN aus. Dort klicken Sie auf COMPUTERSCHUTZ und dann auf die Schaltfläche ERSTELLEN (Abbildung 14.51). Geben Sie eine aussagekräftige Bezeichnung für den Wiederherstellungspunkt ein und klicken Sie auf ERSTELLEN.

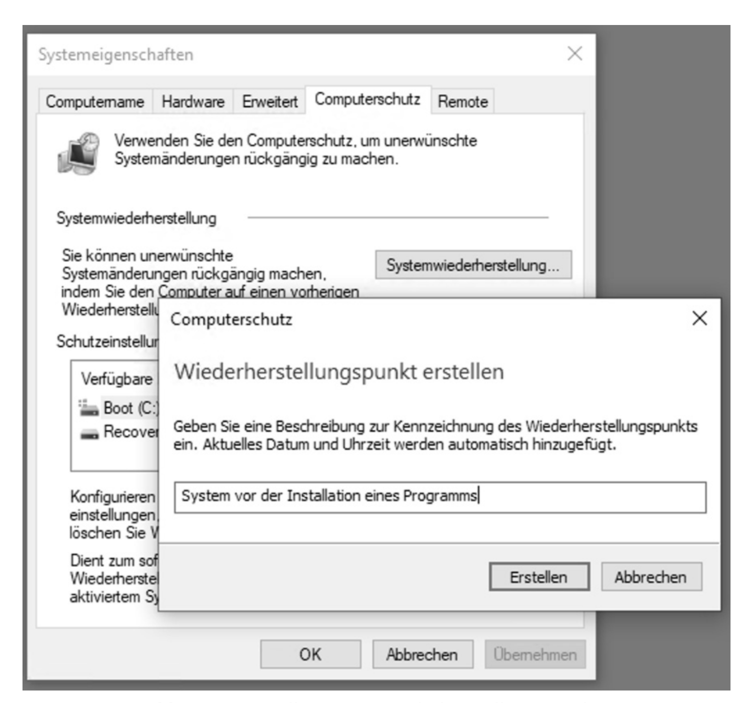


Abb. 14.51: Erstellen eines Wiederherstellungspunkts

Hinweis

In Windows 10 ist die Systemwiederherstellung standardmäßig deaktiviert. Falls Sie eine Systemwiederherstellung vornehmen möchten, dürfen Sie nicht erwarten, Wiederherstellungspunkte vorzufinden. Unter diesen Umständen müssen Sie sich womöglich das Feature DIESEN PC ZURÜCKSETZEN von Windows 10 ansehen, das ich in Kapitel 16 ausführlich erörtere.

Wenn Sie auf der Registerkarte COMPUTERSCHUTZ auf die Schaltfläche SYSTEMWIEDERHERSTELLUNG klicken, werden Sie womöglich überrascht sein, wie viele Wiederherstellungspunkte bereits automatisch erstellt wurden, wenn es sich nicht um einen ganz neuen Rechner handelt (Abbildung 14.52).

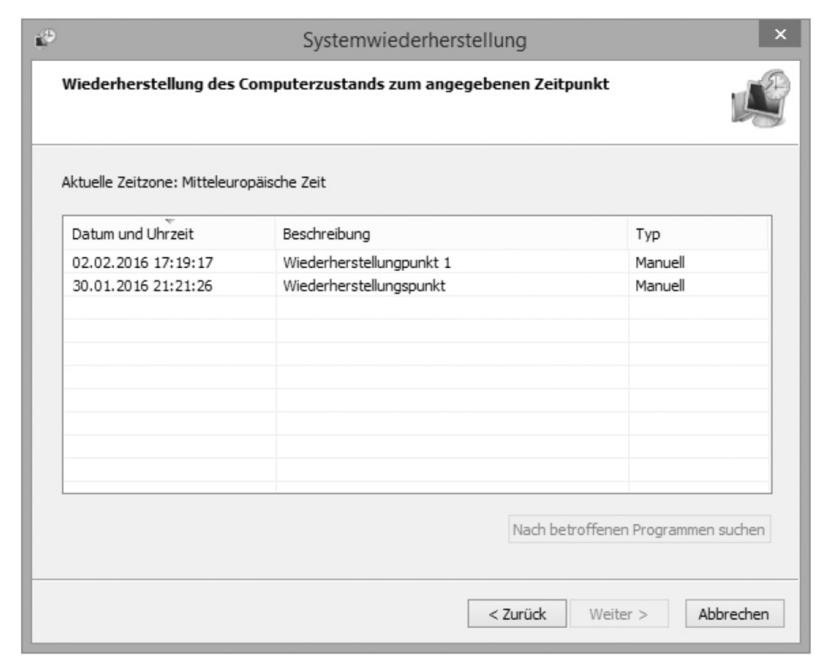


Abb. 14.52: Wiederherstellungspunkte in Windows

Die Systemwiederherstellung erstellt einige Wiederherstellungspunkte automatisch, beispielsweise bei jeder Installation neuer Software. Falls eine solche Installation Schaden auf Ihrem Rechner anrichten sollte, versetzen Sie das System einfach wieder in den Zustand vor der Installation, wodurch der Schaden behoben sein sollte.

Während des Wiederherstellungsvorgangs werden nur Einstellungen und Programme geändert. Daten gehen dabei nicht verloren. Alle Programme und Einstellungen auf dem Rechner werden wieder in den Zustand zum Zeitpunkt der Erstellung des Wiederherstellungspunkts versetzt. Diese Funktion ist für überarbeitete Techniker von unschätzbarem Wert! Durch die einfache Wiederherstellung lassen sich zahlreiche von Benutzern verursachte Fehler beheben.

Um das System anhand eines zuvor angelegten Wiederherstellungspunkts wiederherzustellen, starten Sie den Assistenten zur Systemwiederherstellung durch Auswahl der Schaltfläche SYSTEMWIEDERHERSTELLUNG auf der Registerkarte COMPUTERSCHUTZ im Dialogfeld SYSTEMEIGENSCHAFTEN.

Sie müssen sich nicht darauf verlassen, dass Wiederherstellungspunkte automatisch angelegt werden. Sie können die Systemwiederherstellung jederzeit starten und die Option ERSTELLEN wählen. Das sollten Sie vor allen Änderungen tun, die möglicherweise nicht zur automatischen Erstellung eines Wiederherstellungspunkts führen, wie beispielsweise der manuellen Bearbeitung der Registry.

Die Systemwiederherstellung ist standardmäßig aktiviert (außer in Windows 10) und belegt einen Teil der Festplattenkapazität zum Ablegen der Daten von Wiederherstellungspunkten. Um die Systemwiederherstellung zu deaktivieren oder die dafür vorgesehenen Festplattenkapazitäten zu ändern, klicken Sie mit der rechten Maustaste auf COMPUTER oder DIESER PC, wählen im Kontextmenü EIGENSCHAFTEN und folgen in der Aufgabenliste dem Link COMPUTERSCHUTZ. Klicken Sie dort auf die Schaltfläche KONFIGURIEREN (Abbildung 14.53).

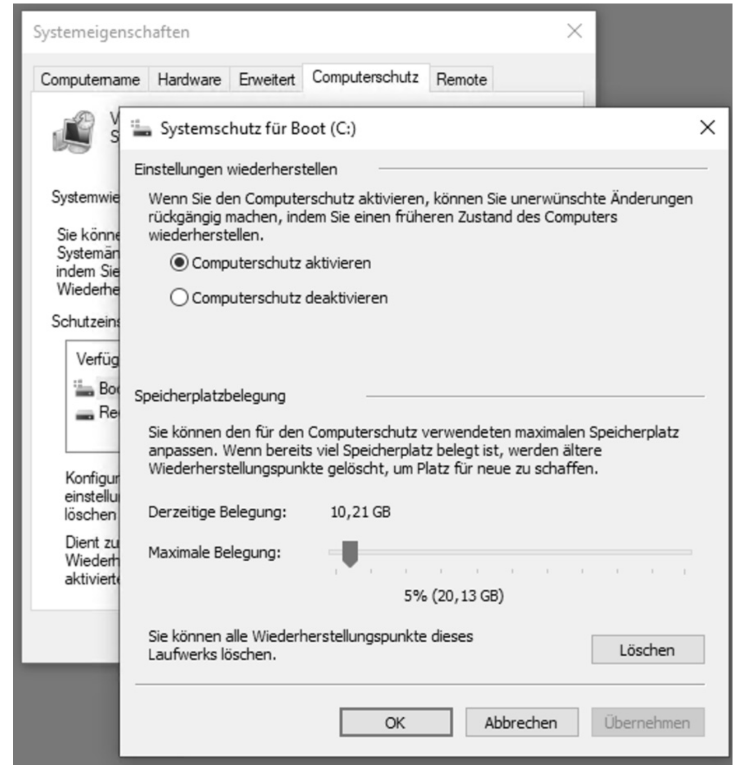


Abb. 14.53: Einstellungen der Systemwiederherstellung und Speicherplatzbelegung

Hinweis

Die Bezeichnungen der Optionen zur Wiederherstellung in Windows 7 unterscheiden sich ein wenig von denen in Windows 10 (Abbildung 14.53) ebenso wie die beschreibenden Texte. Die Funktionalität ist jedoch die gleiche, also ist alles in Ordnung, wenn Sie es mit Datensicherungen von Windows 7 zu tun haben.

14.4 Wiederholung

14.4.1 Fragen

1. Mit welchem Tool können Sie ändern, welche Programme beim Start von Windows 7 geladen werden?
   A. `msstartup`
   B. `msinfo32`
   C. `msconfig`
   D. `ipconfig`
2. Mit welchem Tool können Sie ändern, welche Programme beim Start von Windows 10 geladen werden?
   A. `msstartup`
   B. `msinfo32`

- **C.** `msconfig`
- **D.** Task-Manager

3. Wozu dient das Programm SYSTEMINFORMATIONEN?
   - **A.** Es liefert Ihnen einen Bericht über die Hardwareressourcen, Komponenten und das Softwareumfeld in Ihrem Computer.
   - **B.** Es ermöglicht Ihnen die Auswahl der Programme und Dienste, die beim Starten von Windows automatisch geladen werden.
   - **C.** Es ermöglicht Ihnen die geplante Ausführung von Programmen wie DATENTRÄGERDEFRAGMENTIERUNG, `chkdsk` und anderer Aufgaben.
   - **D.** Es ermöglicht Ihnen die automatische benutzerdefinierte Sicherung Ihrer Dateien und Einstellungen.
4. Mit welchem Tool können Sie ein beschädigtes Windows-Betriebssystem reparieren, indem Sie den Rechner in einen früheren Zustand zurückversetzen?
   - **A.** WINDOWS-WIEDERHERSTELLUNG
   - **B.** WIEDERHERSTELLUNGS-MANAGER
   - **C.** TIME MACHINE
   - **D.** SYSTEMWIEDERHERSTELLUNG
5. Worum handelt es sich bei der Datenausführungsverhinderung (DEP)?
   - **A.** Eine Technologie, die verhindert, dass Viren die Kontrolle über in den Arbeitsspeicher geladene Programme übernehmen
   - **B.** Eine Technologie, mit der Sie unterschiedliche Berechtigungen für verschiedene Benutzer des Rechners setzen können
   - **C.** Eine Technologie, die verhindert, dass Programme auf Ihrem Rechner installiert werden
   - **D.** Eine Technologie, die verhindert, dass Dateien auf Ihre Festplatte geschrieben werden
6. Mit welchem Werkzeug können Sie eine frühere Treiberversion wieder zurückholen, wenn Sie einen Treiber auf Ihrem System installieren, der Probleme verursacht?
   - **A.** TREIBERVERWALTUNG
   - **B.** `msconfig`
   - **C.** GERÄTE-MANAGER
   - **D.** SYSTEMINFORMATIONEN
7. Mit welchem Werkzeug können Sie in Windows Massenspeichergeräte überprüfen und reparieren?
   - **A.** Datenträgerdefragmentierung
   - **B.** Festplattendienstprogramm
   - **C.** Fehlerüberprüfung
   - **D.** Fehlerbehebung
8. Johanna hat sich ein neues Gamepad gekauft und mit dem Hardware-Assistenten installiert, es funktioniert jedoch nicht. Was sollte sie als Nächstes tun? (Wählen Sie zwei Antworten aus.)
   - **A.** Auf den Webseiten des Herstellers nach neuen Treibern suchen
   - **B.** AUTOMATISCHE SYSTEMWIEDERHERSTELLUNG verwenden, um das System wieder in einen funktionsfähigen Zustand zu versetzen
   - **C.** Einen Wiederherstellungspunkt verwenden, um das System wieder in einen funktionsfähigen Zustand zu versetzen
   - **D.** Windows Update ausführen, um nach neuen Treibern zu suchen

9. Welches Tool in macOS dient zum Erstellen vollständiger Backups?
   A. AppleBack
   B. Benutzer & Gruppen
   C. Time Machine
   D. Systemeinstellung SICHERUNGEN
10. Welches zu Windows 8, 8.1 und 10 gehörende Feature ermöglicht es, regelmäßige Sicherungen Ihrer Dateien und Ordner zu erstellen?
   A. Systemkonfiguration
   B. Sichern und Wiederherstellen
   C. AutoPlay
   D. Dateiversionsverlaufs

14.4.2 Antworten

1. **C.** Mit `msconfig` können Sie die Prozesse und Dienste auswählen, die beim Start von Windows 7 geladen werden.
2. **D.** Der Task-Manager ermöglicht es, die Prozesse und Dienste zu ändern, die beim Start von Windows 10 geladen werden.
3. **A.** Das Programm SYSTEMINFORMATIONEN liefert Ihnen eine Fülle von Informationen über Ihr System.
4. **D.** Über SYSTEMWIEDERHERSTELLUNG können Sie den Rechner in einen früheren Zustand zurückversetzen.
5. **A.** Die Datenausführungsverhinderung verhindert, dass Viren die Kontrolle über in den Arbeitsspeicher geladene Programme übernehmen.
6. **C.** Die Option INSTALLIERTER TREIBER/VORHERIGER TREIBER (Driver Rollback) im Geräte-Manager eignet sich hervorragend zur Behebung von Treiberproblemen.
7. **C.** Windows verwendet die Fehlerüberprüfung, um Massenspeichergeräte wie HDDs und SSDs zu überprüfen und zu reparieren.
8. **A, D.** Johanna sollte sowohl auf den Webseiten des Herstellers als auch per Windows Update nach den neuesten Treibern suchen.
9. **C.** macOS verwendet zum Erstellen vollständiger Backups Time Machine.
10. **D.** Der Dateiversionsverlauf ist ein praktisches Werkzeug zum Erstellen von Backups, das zu Windows 8, 8.1 und 10 gehört. Es ermöglicht regelmäßige Sicherungen wichtiger Dateien und Ordner.

Eingabeaufforderung 15

Themen in diesem Kapitel:

- Funktionsweise der Eingabeaufforderung bzw. der Kommandozeile
- Grundlegende Befehle
- Dateioperationen auf der Kommandozeile
- Weitere nützliche Befehle in der Eingabeaufforderung von Windows ausführen
- Weitere nützliche Befehle im Terminal von macOS und Linux
- Skriptsprachen und Plattformen

Wenn ich eine Klasse neuer Techniker unterrichte und zu der Stelle komme, an der mit der Eingabeaufforderung gearbeitet werden soll, dann höre ich unweigerlich immer wieder ein Aufstöhnen und werde mit Fragen und Beschwerden förmlich bombardiert. »Warum sollen wir diesen alten Kram lernen?« »Ist das eine Art geheimnisvoller Ritus zum Quälen von IT-Klassen?«

Für Techniker, die diese Schnittstelle beherrschen, ist die Befehlszeile ein mächtiges, schnelles und elegantes Werkzeug für die Arbeit am PC. Den Umgang mit der Schnittstelle und deren Arbeitsweise zu erlernen, ist für alle Techniker, die über den Anfängerstatus hinauskommen wollen, nicht nur nützlich, sondern unverzichtbar. Sie kommen bei modernen Computern schlicht und einfach nicht ohne die Befehlszeile aus! Und für die CompTIA A+-Zertifizierung müssen Sie etliche Befehle kennen, sowohl für Windows als auch für Linux, mit denen Sie über die Kommandozeile vom Umbenennen von Dateien bis hin zur Wiederherstellung von Systemdateien alle Aufgaben erledigen können.

Wenn Sie neben Windows auch an anderen Betriebssystemen interessiert sind, wie beispielsweise Linux, werden Sie feststellen, dass ein Großteil aller wichtigen Arbeiten von der Kommandozeile aus erledigt wird. Sogar macOS unterstützt eine Kommandozeile.

Für die Beliebtheit der Kommandozeile gibt es drei Gründe: Erstens können Sie die meisten Aufgaben deutlich schneller erledigen, indem Sie einen Textbefehl eingeben, als wenn Sie sich durch eine GUI klicken müssten. Zweitens verlangt eine Befehlszeile dem Betriebssystem kaum Ressourcen ab, deshalb ist sie die Methode der Wahl, wenn Sie keine vollständige GUI für Ihr Betriebssystem brauchen. Drittens können Textbefehle leicht in Skripte eingefügt werden, was es ermöglicht, komplexe Aufgaben zu automatisieren.

Sind Sie nun überzeugt vom Konzept der Eingabeaufforderung? Gut! Dieses Kapitel stellt Ihnen die Kommandozeile unter Windows, macOS und Linux vor, erklärt, wie sie funktioniert und was hinter den Kulissen passiert. Sie lernen die Konzepte und die wichtigsten Befehle kennen und werden dann mit Dateien und Ordnern auf Ihren Laufwerken arbeiten und Skripte erstellen. Um sich den Stoff aus diesem Kapitel anzueignen, probieren Sie am besten jeden der vorgestellten Befehle aus.

Hinweis

Wenn Sie keinen Linux-Rechner besitzen, sollten Sie an dieser Stelle schon mal einen Blick auf Kapitel 22, *Virtualisierung*, werfen und eine virtuelle Maschine auszuprobieren, auf der Sie Linux installieren und testen können. Laden Sie sich unter `www.virtualbox.org` die kostenlose Virtualisierungslösung Oracle VirtualBox und unter `www.ubuntu.com` eine ISO-Datei herunter und probieren Sie es aus!

1002

15.1 Grundlagen der Befehlszeile

Wie also funktioniert eine Kommandozeilenschnittstelle? Es ist ein wenig so, als ob Sie mit dem Computer chatten würden. Der Rechner teilt Ihnen mit, dass er zum Empfang von Befehlen bereit ist, indem er eine bestimmte Zeichenfolge anzeigt, die *Eingabeaufforderung* (*Prompt*) genannt wird. Hier ist ein Beispiel:

```
>: Willst Du spielen?
>: _
```

Sie geben einen Befehl ein (fett gedruckt) und betätigen [↵], um ihn abzusenden:

```
>: Willst Du spielen?
>: Was für ein Spiel?
>: _
```

Der Rechner nimmt sich einen Moment Bedenkzeit und führt den Befehl aus. Wenn er damit fertig ist, dann zeigt er, oft zusammen mit einigen Angaben zu seiner Tätigkeit, eine neue Eingabeaufforderung an:

```
>: Willst Du spielen?
>: Was für ein Spiel?
>: Ein wirklich lustiges Spiel ...
>: _
```

Wenn wieder eine neue Eingabeaufforderung angezeigt wird, bedeutet dies, dass der Rechner auf den nächsten Befehl wartet. Sie geben dem Rechner über die grafische Benutzeroberfläche ebenfalls Befehle, indem Sie Schaltflächen und Menüoptionen mit der Maus anklicken, anstatt sie über die Tastatur einzutippen. Das Ergebnis ist im Grunde genommen dasselbe: Sie teilen dem Rechner mit, was er tun soll, und dieser reagiert darauf.

Tipp: Windows-Programme von der Kommandozeile aus

Bedenken Sie bei der Lektüre dieses Kapitels, dass die Kommandozeile einfach nur eine weitere Möglichkeit zur Kommunikation mit dem Betriebssystem darstellt. Ob Sie nun etwas anklicken oder einen Befehl eingeben: Windows reagiert darauf! Probieren Sie Folgendes: Geben Sie auf der Kommandozeile `notepad` ein und drücken Sie [↵]. Nun startet das grafische Programm EDITOR. Oder geben Sie `explorer` ein und drücken Sie [↵]: Voilà! Der Explorer wird geöffnet. Windows reagiert auf Ihre Befehle.

15.1.1 Shells

Die Kommandozeile bietet eine weitere Möglichkeit, um mit dem Betriebssystem zu kommunizieren. Sie nimmt Eingaben entgegen und übermittelt sie an das Betriebssystem in einer Form weiter, die es verarbeiten kann. Dann wird das Ergebnis angezeigt. Das Programm, das die Eingaben entgegennimmt, wird als *Kommandozeileninterpreter* oder *Shell* bezeichnet. Unter Windows ist `cmd.exe` die Standard-Shell. macOS und die meisten Linux-Distributionen verwenden als Standard-Shell `bash`. Die meisten Betriebssysteme verfügen über nur eine grafische Benutzeroberfläche, aber für Shells gilt das nicht. Alle Betriebssysteme können problemlos auch andere Shells verwenden. Auf macOS und

Linux kann `bash` leicht durch eine andere der verbreiteten Shells ersetzt werden, wie etwa Z-Shell (zsh), Korn-Shell (ksh) oder C-Shell (csh). Unter Windows können Sie statt `cmd.exe` die PowerShell verwenden. Computerfreaks liegt es im Blut, mit diesen alternativen Shells herumzuexperimentieren.

Hinweis

Wenn Sie eine Eingabeaufforderung bzw. ein Terminal öffnen, wird eine Shell gestartet, die als Kommandozeileninterpreter fungiert. In diesem Kapitel bleiben wir bei den gebräuchlichsten Shells und verwenden sie auf typische Weise. Sie sollten jedoch wissen, dass Shells austauschbar und hochgradig konfigurierbar sind.

15.1.2 Zugriff auf die Befehlszeile in Windows

In Windows greifen Sie auf die Befehlszeile zu, indem Sie das Programm `cmd.exe` starten. In Kapitel 2, *Der gläserne PC*, haben wir dieses Thema schon kurz gestreift, aber hier sehen wir uns den Vorgang etwas genauer an.

Üblicherweise verwendet man das Startmenü oder das Suchfeld des Startbildschirms, um auf die Befehlszeile zuzugreifen. Geben Sie im Suchfeld des Startmenüs `cmd` ein und drücken Sie [↵], um die Eingabeaufforderung zu starten (Abbildung 15.1).

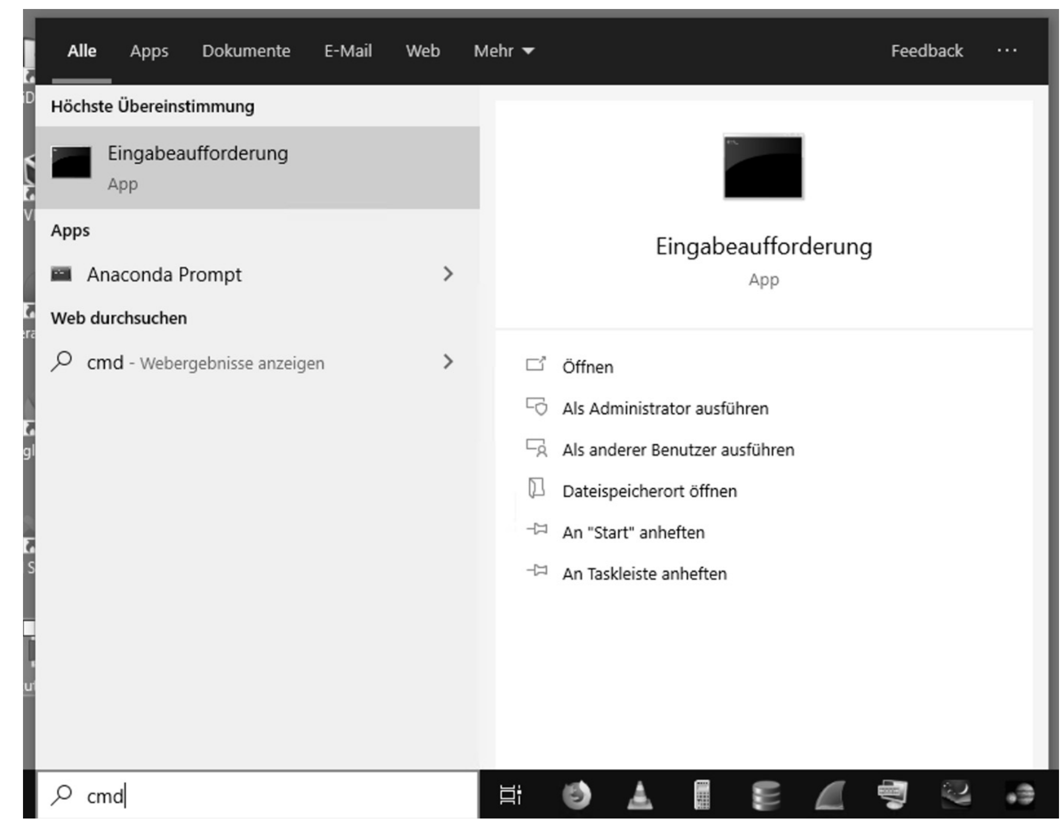


Abb. 15.1: Starten der Eingabeaufforderung in Windows 10

Nun erscheint das Fenster EINGABEAUFFORDERUNG mit schwarzem Hintergrund und weißer Schrift auf dem Bildschirm – willkommen auf der Kommandozeile! Zum Schließen dieses Fensters können Sie wie bei allen anderen Fenstern auch, die Schaltfläche in der oberen rechten Ecke verwenden, oder Sie geben den Befehl `exit` ein und drücken ↵ (Abbildung 15.2).



Abb. 15.2: Eingabeaufforderung in Windows 8.1

Wenn Sie versuchen, einen Befehl auf der Kommandozeile auszuführen, für den erhöhte Rechte oder Administratorrechte erforderlich sind, meldet sich die BENUTZERKONTENSTEUERUNG (die Sie aus Kapitel 13 bereits kennen) mit dem Dialogfeld »Möchten Sie zulassen, dass ...«. Sie können einen Befehl auch manuell mit erhöhten Rechten ausführen, indem Sie mit der rechten Maustaste auf eine Verknüpfung mit der Eingabeaufforderung klicken und im Kontextmenü ALS ADMINISTRATOR AUSZUFÜHREN wählen. Wenn Sie aufgefordert werden, ein Kennwort oder Anmeldedaten einzugeben, tippen Sie die erforderlichen Informationen ein, um fortzufahren.

Hinweis

Um eine Verknüpfung mit der Eingabeaufforderung zu erstellen, gehen Sie wie folgt vor: Klicken Sie den Desktop mit der rechten Maustaste an und wählen Sie NEU|VERKNÜPFUNG. Geben Sie für den Speicherort des Elements `cmd` ein und klicken Sie auf WEITER. Geben Sie als Namen für die Verknüpfung ebenfalls `cmd` ein und klicken Sie auf FERTIG STELLEN. Nun erscheint die Verknüpfung auf dem Desktop. Klicken Sie mit der rechten Maustaste darauf, öffnen Sie das Dialogfeld EIGENSCHAFTEN und klicken Sie auf der Registerkarte VERKNÜPFUNG auf die Schaltfläche ERWEITERT. Aktivieren Sie das Kontrollkästchen ALS ADMINISTRATOR AUSFÜHREN und klicken Sie zweimal auf OK, um die Änderung zu speichern. Sie haben nun eine Verknüpfung zur Eingabeaufforderung erstellt, die immer mit Administratorrechten ausgeführt wird. (Die beschriebenen Schritte gelten für Windows 10, aber das funktioniert unter Windows 7/8/8.1 ebenfalls, auch wenn die Dialogfelder etwas anders aussehen.)

15.1.3 Zugriff auf die Befehlszeile in macOS und Linux

Die Kommandozeile funktioniert in macOS und in Linux praktisch auf dieselbe Art und Weise. Das ist nicht weiter überraschend, da beide Systeme auf UNIX beruhen. Der Terminalemulator in macOS heißt schlicht und einfach *Terminal*. Die vielen verschiedenen Linux-Distributionen verwenden auch unterschiedliche Emulatoren, wie z.B. *Konsole* oder das *Gnome-Terminal*. Um das Ganze etwas zu vereinfachen, verwende ich die Kommandozeile in Ubuntu, die praktischerweise ebenfalls den Namen *Terminal* trägt.

Das Terminal in macOS können Sie per Doppelklick auf das Programmsymbol im Ordner PROGRAMME|DIENSTPROGRAMME öffnen, oder Sie verwenden Spotlight (⌘ + Leertaste), tippen `terminal` ein und drücken ↵ (Abbildung 15.3).

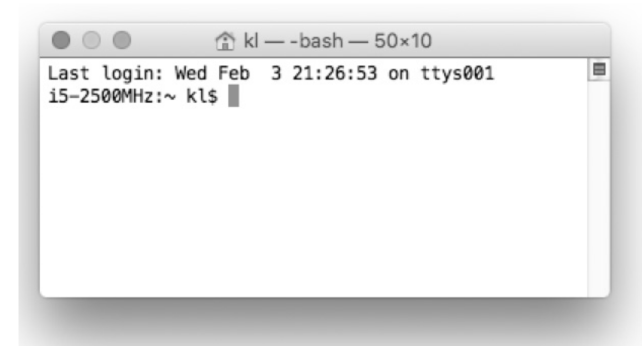


Abb. 15.3: Terminal in macOS

Wichtig

Spotlight ist ein phänomenales Suchwerkzeug in macOS. Es indiziert die Laufwerke, aber nicht nur die Dateinamen, sondern auch die Inhalte. Das bedeutet, Sie können (natürlich) nicht nur nach Dateien suchen, sondern auch nach Apps, E-Mails, Musik, Kontakten und sogar Verkehrsinformationen. Probieren Sie es aus!

Die Methode zum Öffnen des Terminals in Linux hängt von der verwendeten Distribution ab. Alle Distributionen mit einer grafischen Benutzeroberfläche bringen irgendein Werkzeug zum Suchen mit, das auf ähnliche Art und Weise funktioniert wie die entsprechenden Werkzeuge in macOS und Windows. Benutzen Sie dieses Tool und geben Sie `terminal` ein, um das Programm zu starten. Daraufhin erscheint ein Terminalfenster wie in Abbildung 15.4.

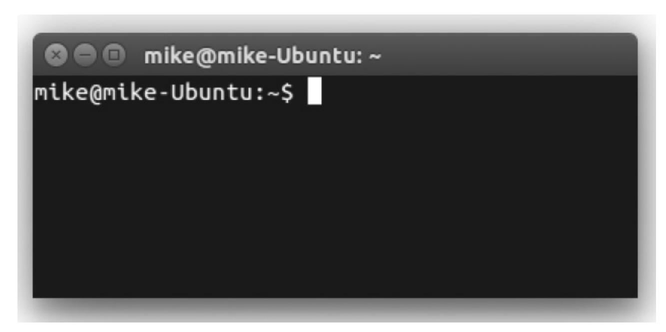


Abb. 15.4: Terminal in Ubuntu

Sowohl macOS als auch Linux gestatten es, Befehle auf der Kommandozeile mit erhöhten Rechten auszuführen, die als *Superuser-* oder *root-Rechte* bezeichnet werden. Die root-Rechte in macOS und Linux entsprechen den erhöhten Rechten in Windows, die Handhabung geschieht jedoch auf unterschiedliche Weise. Öffnen Sie ein Terminalfenster und geben Sie zur Ausführung eines Befehls mit root-Rechten vor dem auszuführenden Kommando `sudo` ein. Das System führt dann nach Abfrage des Kennworts den eingegebenen Befehl mit root-Rechten aus.

Falls der Befehl `sudo` auf einem System nicht verfügbar ist, sollte es den älteren Vorgänger `su` geben. Man gibt typischerweise `su` ein und drückt [↵]. Nach erfolgreicher Eingabe des Kennworts ändert sich der Prompt. (Für gewöhnlich wird am Ende des Prompts statt eines $-Zeichens das Zeichen # angezeigt). Alle nachfolgend eingegebenen Befehle werden nun mit root-Rechten ausgeführt. Wenn Sie Ihre Aufgaben erledigt haben, geben Sie `exit` ein und drücken [↵]. Dadurch wird das Terminalfenster nicht wie sonst geschlossen, stattdessen kehren Sie zurück zu einer »normalen« Kommandozeile. Sehen Sie sich das folgende Beispiel an:

```
mike@server:~$ su
Password:_
root@server:/home/mike# exit
mike@server:~$
```

Wichtig

Auf vielen Linux-Systemen ist das root-Benutzerkonto aus Sicherheitsgründen deaktiviert. In diesem Fall funktioniert der Befehl `su` nicht. Der Befehl `sudo` erlaubt es Benutzern, Kommandos mit root-Rechten auszuführen, ohne dass ihnen das root-Kennwort bekannt ist.

15.1.4 Die Befehlszeile verwenden

Bei der Verwendung der Befehlszeile ist immer ein bestimmtes Verzeichnis *aktiv*, das sogenannte Arbeitsverzeichnis, das oft in der Eingabeaufforderung angezeigt wird. Dies ist deshalb von Bedeutung, weil sich alle eingegebenen Befehle auf die Dateien des gerade aktiven Verzeichnisses beziehen. Wenn Sie z.B. eine Eingabeaufforderung wie die folgende sehen, können Sie daran erkennen, dass das Stammverzeichnis des Laufwerks `C:` aktiv ist:

```
C:>
```

Die Eingabeaufforderungen in macOS und in Linux unterscheiden sich ein wenig von der in Windows, die Funktionalität ist jedoch dieselbe. Zunächst einmal gibt es in macOS und Linux keine Laufwerksbuchstaben. Alle Speichergeräte werden einfach nur als Ordner angezeigt. Darüber hinaus zeigt die Linux-Eingabeaufforderung in der Regel den Namen des aktuell angemeldeten Benutzers, den Rechnernamen sowie das aktuelle Arbeitsverzeichnis an. Und schließlich verwenden macOS und Linux den normalen Schrägstrich (/) anstatt des umgekehrten Schrägstrichs (\). Die nachstehende Eingabeaufforderung besagt, dass an einem Rechner namens »server« der Benutzer »mike« angemeldet ist, dessen Arbeitsverzeichnis der Ordner »home« ist:

```
mike@server:/home$
```

Wenn Sie in Windows eine Eingabeaufforderung wie in Abbildung 15.5 sehen, dann wissen Sie, dass das Verzeichnis `C:\Diplom\APLUS\` auf dem Laufwerk `C:` aktiv ist. Der Trick besteht daher darin, erst einmal das Laufwerk und das Verzeichnis zu aktivieren, von dem aus gearbeitet werden soll.

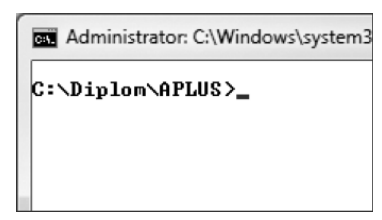


Abb. 15.5: Hier verweist die Eingabeaufforderung auf das aktive Verzeichnis `C:\Diplom\APLUS`.

15.1.5 Terminal beenden

Das Beenden der Kommandozeile ist einfach und geschieht unter Windows und in macOS bzw. Linux auf dieselbe Art und Weise. Geben Sie `exit` ein und drücken Sie [↵]. Das Terminalfenster wird daraufhin geschlossen.

```
mike@server:/home$ exit
```

15.1.6 Dateinamen und Dateiformate

Bei der Verwendung der Kommandozeile ist Präzision erforderlich. Das bedeutet, dass Befehle, Dateinamen und Befehlsoptionen akribisch genau eingegeben werden müssen. Anderenfalls kommt es zu Fehlern oder zu gar keinem Ergebnis. Was Sie eingeben (oder falsch eingeben), kann in der Befehlszeile enorme Auswirkungen haben.

Das Betriebssystem betrachtet sämtliche Programme und Daten als individuelle *Dateien*, die auf einem Massenspeichergerät im Binärformat abgelegt sind, aber jedes Programm verwendet eine eigene Methode zur Organisation dieser Binärdateien. Man spricht dann von dem Dateiformat. Ein Programm kann die Dateien eines anderen Programms nicht lesen, wenn es nicht in der Lage ist, das Dateiformat in sein eigenes Format zu konvertieren.

Jede Datei besitzt einen Namen, der zusammen mit der Datei auf dem Laufwerk gespeichert wird. Die Namen bestehen aus zwei Teilen, nämlich dem eigentlichen Dateinamen und der Erweiterung. In der Anfangszeit des PCs verwendete Microsoft ein Dateisystem, das vorschrieb, dass der Dateiname maximal acht Zeichen lang sein durfte. Die optionale Erweiterung konnte maximal drei Zeichen lang sein. Der Dateiname und die Erweiterung sind durch einen Punkt (*dot*) voneinander getrennt. Hier ein Beispiel für einen derartigen Dateinamen:

```
rechnung.txt
```

Die Einschränkungen dieses »8.3«-Namensformats gelten für moderne Betriebssysteme natürlich nicht mehr. Hier sind einige Beispiele gültiger Dateinamen:

`franz.exe`	`ErsterVersuch.aes`	`datei1.erweiterung`
`treiber3.h`	`Johanna mag lange Dateinamen.doc`	`KeineErweiterung`

Egal, ob Sie Windows, macOS oder Linux einsetzen, die Dateinamenerweiterungen sind immer sehr wichtig, weil die Erweiterung dem Computer den Typ oder die Funktion einer Datei mitteilt. Die Erweiterung weist üblicherweise darauf hin, zu welchem Programm die jeweilige Datendatei gehört. Beispielsweise verwendet Microsoft Word Dateien mit der Erweiterung `.docx` oder `.doc`, während PowerPoint `.pptx` oder `.ppt` als Erweiterung benutzt. Die Erweiterungen von Bilddateien verweisen hingegen häufig auf das Format, das zur Speicherung der Datei verwendet wurde, wie z.B. `.gif` (CompuServes Graphics Interchange Format) oder `.jpg` für JPEGs (Joint Photographic Experts Group). Abbildung 15.6 zeigt die Zuordnung von `.png`-Dateien zu einem Programm.

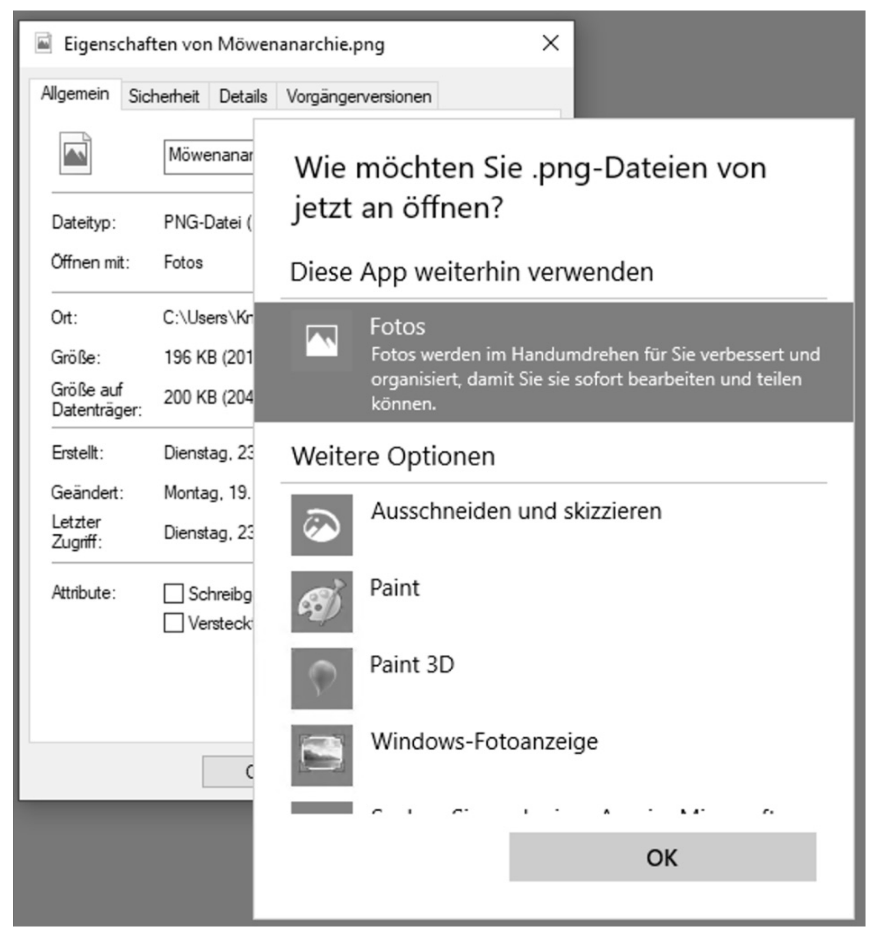


Abb. 15.6: Zuordnung von Dateien zu einem Programm

Hinweis

Alle Betriebssysteme gestatten es, Dateien bestimmten Programmen zuzuordnen. Wenn Sie `.docx`-Dateien von Microsoft Office statt mit Word lieber mit LibreOffice öffnen möchten, ist das problemlos möglich.

Durch Änderung der Namenerweiterung einer Datendatei wird zwar deren Inhalt nicht geändert, aber ohne die richtige Erweiterung weiß Ihr Betriebssystem nicht, welchem Programm es die Datendatei zuordnen soll. Dies sehen Sie deutlich im Explorer. Abbildung 15.7 zeigt einen Ordner, der zwei identische Bilddateien enthält. Die rechte wird als Miniatur angezeigt, da Windows erkennt, dass es sich um eine JPEG-Bilddatei handelt. Die linke Datei wird als allgemeines Symbol dargestellt, weil ich die Dateinamenerweiterung gelöscht habe. Windows zeigt die Dateinamenerweiterung standardmäßig nicht an, macOS und die meisten Linux-Distributionen hingegen schon.

Dateiname und Erweiterung spielen auch bei Verwendung der Kommandozeile eine wichtige Rolle, weil Sie wissen müssen, auf welche Art von Datei Sie zugreifen, wenn Sie einen Befehl eingeben. Die Eingabe bestimmter Dateinamen kann beispielsweise dazu führen, dass das Betriebssystem ein Pro-

gramm startet oder eine Reihe von Befehlen ausführt. Mehr zu ausführbaren Dateien in Abschnitt 15.1.15, *Programme starten in Windows*.

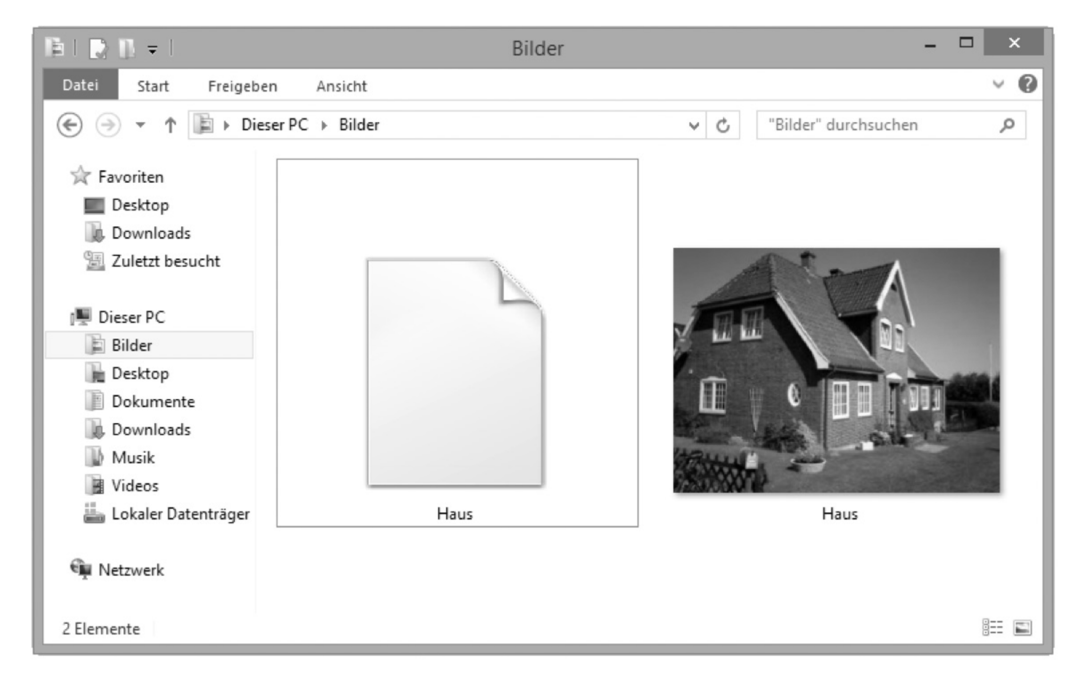


Abb. 15.7: Datei ohne Dateinamenerweiterung

15.1.7 Laufwerke und Ordner

Bei der Arbeit an der Befehlszeile müssen Sie bestimmte Laufwerke und Ordner aktivieren können, in denen sich die Dateien oder Programme befinden, mit denen Sie arbeiten wollen. Das ist manchmal komplizierter, als man denkt.

Ich möchte nun kurz zusammenfassen, was Sie bereits aus Kapitel 9, *Vorbereitung und Wartung von Festplatten*, wissen. Windows weist allen Festplattenpartitionen (außer der Systempartition) und erkannten Massenspeichergeräten Laufwerksbuchstaben zu. Festplattenpartitionen werden Buchstaben beginnend mit `C:` zugeordnet. Optischen Laufwerken wird standardmäßig der nächste nach der letzten Festplattenpartition freie Laufwerksbuchstabe zugeordnet. Darüber hinaus können Sie sogar komplette Festplatten als Bereitstellungspunkte in ein anderes Laufwerk einhängen.

macOS und Linux kennen keine Laufwerksbuchstaben. Stattdessen wird die Startpartition zum Stammverzeichnis, das nur durch einen Schrägstrich / repräsentiert wird. Alle weiteren Speichergeräte (Partitionen, optische Laufwerke, USB-Sticks usw.) werden in das System »eingehängt« (»gemountet«) und das Betriebssystem behandelt sie wie Ordner. Diese Ordner befinden sich meistens in einem eigenen Verzeichnis auf dem Startlaufwerk, das unter Linux `/mount` oder `/media` und in macOS `/Volumes` heißt.

Wie die Laufwerke nun genau heißen, spielt letzten Endes keine Rolle, denn alle Betriebssysteme verwenden unabhängig von den Laufwerksnamen zur Organisation der Laufwerksinhalte einen hierarchischen Verzeichnisbaum. Alle Dateien werden in Gruppen zusammengefasst, die *Ordner* genannt werden. Techniker verwenden häufig den Begriff *Verzeichnis* anstelle von Ordner, meinen damit aber dasselbe. Alle Dateien, die sich nicht in einem Ordner innerhalb der Baumstruktur befinden, befinden sich in der *Wurzel* (root) des Verzeichnisbaums, dem *Stamm-* bzw. *Hauptverzeichnis*. Innerhalb von Ver-

zeichnissen kann es wiederum weitere Verzeichnisse geben. Ordner innerhalb anderer Ordner werden Unterverzeichnis oder auch Unterordner genannt. Ein Ordner kann viele Unterverzeichnisse haben. In verschiedenen Ordnern können Dateien mit demselben Namen existieren, jedoch kann es keine zwei Dateien in ein und demselben Ordner mit demselben Namen geben. Genauso dürfen zwei Unterverzeichnisse nicht denselben Namen haben, sofern sie sich im selben Ordner befinden.

Hinweis

Es ist hilfreich, sich die Ordnerstruktur als einen auf dem Kopf stehenden Baum vorzustellen, weil sich in der Fachsprache die Wurzel bzw. das Stammverzeichnis »über« den Ordnern befindet, in das es aufgeteilt ist, und sich die Unterordner »unter« dem Stammverzeichnis »über« den darin enthaltenen Unterordnern befinden. Beispielsweise sagt man, dass die Datei im Ordner Adobe unter Programme zu finden ist.

In Windows sprechen Sie ein Laufwerk über dessen Laufwerksbuchstaben und einen nachgestellten Doppelpunkt an. Die Festplatte lässt sich z.B. mit `C:` ansprechen. Das Stammverzeichnis der Festplatte sprechen Sie mit dem Backslash (»\«) nach dem `C:` an (`C:\`). Ein bestimmtes Verzeichnis sprechen Sie an, indem Sie dessen Namen hinzufügen, beispielsweise `C:\Test` für das Verzeichnis `Test` im Stammverzeichnis auf dem Festplattenlaufwerk `C:`. Unterverzeichnisse eines Verzeichnisses werden durch Hinzufügen eines Backslashs und ihres Namens angesprochen. Wenn das Verzeichnis `Test` ein Unterverzeichnis namens `System` enthält, wird dieses folgendermaßen angegeben: `C:\Test\System`. Mit dieser Art der Namensgebung lassen sich Speicherort und Name beliebiger Dateien vollständig beschreiben. Wenn das Verzeichnis `C:\Test\System` eine Datei namens `test2.txt` enthält, lautet deren vollständiger Name `C:\Test\System\test2.txt`.

Der genaue Speicherort einer Datei wird *Pfadname* genannt. Der Pfadname für `test2.txt` lautet `C:\Test\System`. Weitere Beispiele für mögliche Pfadnamen sind:

```
C:\Program Files
C:\Users\mike\Desktop
F:\FRUSCH3\CLEAR
D:\
```

macOS und Linux verwenden ebenfalls Pfade, allerdings wird zum Trennen der Ordnernamen ein normaler Schrägstrich (/) statt des umgekehrten (\) benutzt. Windows und macOS unterscheiden außerdem bei Datei- und Ordnernamen nicht zwischen Groß- und Kleinschreibung, Linux hingegen schon. Linux gestattet es beispielsweise, zwei Ordner namens »Mike« und »mike« im selben Verzeichnis anzulegen. Windows erlaubt dies nicht. Hier sind weitere Beispiele für Pfadnamen in macOS und Linux:

```
/usr/local/bin
/Programme/Dienstprogramme
/home/mike/Desktop
```

In macOS und Linux wird das Arbeitsverzeichnis in der Eingabeaufforderung ein wenig anders als in Windows dargestellt. Das Arbeitsverzeichnis verweist generell auf den Ordner /Users/<Benutzername> (macOS) bzw. /home/<Benutzername> (Linux). macOS und Linux zeigen stattdessen standardmäßig nur eine Tilde (~) an:

```
mike@server:~$
```

Die Tilde ist ein Kürzel für das Heimverzeichnis des Benutzers. Das Arbeitsverzeichnis ist in diesem Fall also `/home/mike`. Sie finden das ein wenig verwirrend? Willkommen in UNIX! macOS und

Linux stellen ein praktisches Hilfsprogramm namens `pwd` bereit, das Ihnen das Arbeitsverzeichnis anzeigt, falls Sie sich nicht sicher sind:

```
mike@server:~$ pwd
/home/mike
```

Wichtig

Die Befehle `pwd` und `passwd` gehören zu den Lernzielen der CompTIA A+-Zertifizierungsprüfung. `pwd` haben Sie soeben kennengelernt. `passwd` wird später in diesem Kapitel noch erläutert.

Es folgt eine Liste von Dingen, die Sie sich hinsichtlich Datei- und Ordnernamen merken sollten:

- Datei- und Ordnernamen können Leerzeichen enthalten.
- In Windows sind die folgenden elf Zeichen nicht erlaubt: * " / \ [ ] : ; | = und ,
- In macOS und Linux ist das einzige nicht erlaubte Zeichen der Schrägstrich: /
- Dateinamenerweiterungen sind nicht unbedingt erforderlich, aber in vielen Fällen kann das Betriebssystem einer Datei beim Fehlen einer solchen kein Programm zuordnen, mit dem sie sich öffnen lässt.

15.1.8 Grundlegende Befehle

Nun ist es an der Zeit, die Eingabeaufforderung auch zu benutzen. Zuvor aber ein warnender Hinweis: Die Kommandozeile ist ziemlich pingelig und unnachgiebig. Sie führt aus, was Sie *eingeben*, nicht, was Sie *meinen* – ein falscher Befehl kann dazu führen, dass wichtige Daten ohne Vorwarnung verloren gehen. Überprüfen Sie den eingegebenen Befehl also lieber doppelt, bevor Sie ↵ betätigen, um ihn auszuführen. In diesem Abschnitt werden Sie erst den Aufbau von Befehlen kennenlernen und sich dann mit vier Befehlen befassen, die zum Navigieren in der Dateistruktur und zu deren Bearbeitung dienen.

Wichtig

Die CompTIA A+-Zertifizierung prüft Ihr Wissen darüber, wann bestimmte Befehle in Windows, macOS oder Linux einzusetzen sind. In den Lernzielen ist angegeben, unter welchen Umständen ein bestimmtes Werkzeug eines Betriebssystems zu verwenden ist. Das ist auch völlig angemessen. Techniker müssen wissen, wann sie ein bestimmtes Werkzeug benötigen, insbesondere bei Verwendung der Befehlszeile.

In diesem Kapitel wird davon ausgegangen, dass Sie erkennen, wann der Gebrauch eines bestimmten Werkzeugs auf der Hand liegt. Wann verwendet man einen Befehl zum Löschen von Dateien? Natürlich, wenn man eine Datei löschen möchte. Falls ein Werkzeug einer ausführlicheren Erläuterung bedarf, wird es erklärt. Rechnen Sie mit Prüfungsfragen, die sich auf die Verwendung der Befehlszeile unter vorgegebenen Umständen beziehen.

15.1.9 Befehlsstruktur: Syntax und Schalter

Alle Befehle der Kommandozeile besitzen einen ähnlichen Aufbau und werden auf dieselbe Weise ausgeführt. Sie geben den Namen des Befehls ein, dem Quelle und/oder Ziel des Befehls und anzuwendende Befehlsmodifikationen folgen. Die Modifikationen werden dadurch aktiviert, dass zusätzliche Zeichen am Ende der Befehlszeile angefügt werden, die *Schalter* oder *Optionen* genannt werden und denen abhängig vom jeweiligen Befehl das Ziel folgen kann. Die formal richtige Schreibweise eines Befehls wird als *Syntax* bezeichnet. Sie müssen bei der Eingabe der Befehle also äußerst genau aufpas-

sen und können nicht das Zeichen »\« verwenden, wenn ein »/« erforderlich ist. Die Befehlszeile ist in dieser Hinsicht absolut unflexibel, Sie müssen also die korrekte Syntax für jeden Befehl kennen.

```
[Befehl] [Ziel (falls vorhanden)] [Schalter]
```

oder

```
[Befehl] [Schalter] [Ziel (falls vorhanden)]
```

Woher wissen Sie, welche Schalter unterstützt werden? Woher wissen Sie, ob die Schalter vor oder nach dem Ziel stehen sollen? Wenn Sie die Syntax und die Schalter für einen bestimmten Befehl erfahren wollen, geben Sie in Windows den Befehl gefolgt von `/?` ein, um Hilfe zu erhalten.

```
[Befehlsname] /?
```

In macOS oder Linux geben Sie den Befehl `man` (für engl. manual, Handbuch) gefolgt von einem Leerzeichen und dem Befehlsnamen ein:

```
man [Befehlsname]
```

Wenn Sie die Beschreibung gelesen haben, können Sie durch Drücken von [Q] wieder zur Kommandozeile zurückkehren.

15.1.10 Verzeichnisinhalte anzeigen: dir und ls

Der Windows-Befehl `dir` bzw. der Befehl `ls` (macOS und Linux) dient zur Anzeige des Inhalts des Arbeitsverzeichnisses.

`dir` und `ls` sind wohl diejenigen Befehle, die auf der Kommandozeile am häufigsten benutzt werden. Wenn Sie unter Windows ein Fenster mit einer Eingabeaufforderung öffnen, dann ist Ihr Benutzerordner aktiv. Das können Sie daran erkennen, dass die Eingabeaufforderung z.B. `C:\Benutzer\Benutzername>` lautet. Geben Sie `dir` ein und drücken Sie [↵]. (Sie müssen alle Befehle an der Eingabeaufforderung mit [↵] abschließen, um diese auszuführen.) Nun sollte die Ausgabe ungefähr so aussehen:

```
:\Users>dir
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: 92AC-B31E

 Verzeichnis von C:\Users

28.01.2016  17:05    <DIR>          .
28.01.2016  17:05    <DIR>          ..
31.01.2016  19:51    <DIR>          Mike
22.08.2013  09:17    <DIR>          Public
28.01.2016  17:05    <DIR>          Susi Sonntag
               0 Datei(en),              0 Bytes
               5 Verzeichnis(se), 119.911.022.592 Bytes frei

C:\Users>
```

Die in Linux voreingestellte Eingabeaufforderung zeigt den vollständigen Pfad nicht an, daher liefert die Eingabe von `ls` im Arbeitsverzeichnis `/home/mike` auf meinem Ubuntu-System folgende Ausgabe:

```
mike@server:~$ ls
Desktop     Downloads  Public     Videos
Documents   photo.jpg  timmy.doc
mike@server:~$
```

Falls Sie diesen Befehl wirklich am Rechner eingeben, denken Sie bitte daran, dass verschiedene PCs auch verschiedene Dateien enthalten, sodass die Anzeige bei Ihnen sicherlich von der obigen abweichen wird. Wenn sehr viel Text zu schnell auf dem Bildschirm ausgegeben wird, können Sie den Befehl `dir /p` (Pause) eingeben. Drücken Sie danach wieder ↵. Der Befehl `dir /p` ist unerhört wichtig, wenn Sie in einem umfangreichen Verzeichnis nach einer bestimmten Datei suchen. Drücken Sie zur Anzeige des nächsten Bildschirms jeweils `Leertaste`.

In macOS und Linux können Sie das Gleiche erreichen, indem Sie `ls | more` eingeben. Das Symbol »|« heißt *Pipe*. Sie weisen das Betriebssystem damit an, die Ausgabe des Befehls `ls` nicht direkt auf dem Bildschirm auszugeben, sondern sie (wie Wasser durch ein Rohr) an den zweiten Befehl namens `more` umzuleiten. Den Pipe-Befehl gibt es in allen drei Betriebssystemen und er ist enorm leistungsfähig. Auf den Pipe-Befehl komme ichspäter in diesem Kapitel noch ausführlich zurück.

Bei manchen Befehlen spielt es keine Rolle, ob Sie trennende Leerzeichen eingeben oder nicht. So liefert beispielsweise die Eingabe von `dir/p` und `dir /p` dieselbe Ausgabe. Bei einigen Befehlen ist es jedoch *erforderlich*, Leerzeichen zwischen Befehl und Schaltern einzugeben.

Sie sollten sich generell angewöhnen, Leerzeichen einzugeben. Dann werden Sie auch nicht auf Probleme stoßen.

Hinweis

Zusätzlich hinter einem Befehl eingetippter Text wie z.B. `/p` oder `/w` nach `dir`, wird *Schalter* genannt. Nahezu alle Schalter können miteinander kombiniert eingesetzt werden und Befehle entsprechend modifizieren. Probieren Sie doch einmal den Befehl `ls -a -l -h` in macOS oder Linux aus!

Bei vielen Befehlen können Sie mehrere Schalter direkt hintereinander angeben. Anstelle des obigen Befehls hätten Sie auch `ls -alh` verwenden können.

Der Befehl dir

Bei Eingabe des einfachen `dir`-Befehls erhalten Sie Einträge, die etwa so aussehen:

```
09.04.2010  17:51           63.664 bambi.jpg
```

Alle diese Einträge beziehen sich auf Dateien. Der `dir`-Befehl führt das Erstellungsdatum, die Erstellungszeit, die Dateigröße in Byte, den Dateinamen und die Dateinamenerweiterung auf. Einträge der folgenden Form sind Ordner:

```
05.04.2009  22:18       <DIR>          Windows
```

Der `dir`-Befehl gibt das Erstellungsdatum, die Erstellungszeit, `<DIR>` als Kennzeichner für den Ordner und den Ordnernamen aus.

Geben Sie jetzt den Befehl `dir /w` ein. Beachten Sie, dass `dir /w` nur die Dateinamen anzeigt, jedoch in fünf Spalten angeordnet. Anschließend geben Sie `dir /?` ein, um die Ausgabe von Abbildung 15.8 zu erhalten, in der alle vom Befehl unterstützten Schalter aufgeführt werden.

```
Auswählen Eingabeaufforderung

C:\Users>dir /?
Listet die Dateien und Unterverzeichnisse eines Verzeichnisses auf.

DIR [Laufwerk:][Pfad][Dateiname] [/A[[:]Attribute]] [/B] [/C] [/D] [/L] [/N]
  [/O[[:]Folge]] [/P] [/Q] [/R] [/S] [/T[[:]Zeit]] [/W] [/X] [/4]

  [Laufwerk:][Pfad][Dateiname]
              Bezeichnet Laufwerk, Verzeichnis und/oder Dateien.

  /A          Listet Dateien mit angegebenen Attributen auf.
  Attribute    D Verzeichnisse        R Schreibgeschützte Dateien
               H Versteckte Dateien   A Zu archivierende Dateien
               S Systemdateien        I Nicht indizierte Dateien
               L  Analysepunkte       - vorangestellt kehrt die Bedeutung um.
  /B          Einfaches Format (keine Kopfdaten, keine Zusammenfassung).
  /C          Zeigt das Tausendertrennzeichen bei Dateigrößen an (Standard-
              einstellung). Verwenden Sie /-C, um das Tausendertrennzeichen
              nicht anzuzeigen.
  /D          Gleich wie Breitformat, jedoch nach Spalten sortiert.
  /L          Verwendet Kleinschreibung.
  /N          Neues, langes Listenformat (Dateinamen auf der rechten Seite).
  /O          Gibt die Liste sortiert aus.
  Folge        N Name (alphabetisch)        S Größe (kleinere zuerst)
               E Erweiterung (alphabetisch) D Datum/Zeit (ältere zuerst)
               G Verzeichnisse zuerst       - vorangestellt kehrt die
                                              Reihenfolge um
  /P          Pausiert nach jeder vollen Bildschirmseite.
  /Q          Gibt den Besitzer der Datei aus.
  /R          Zeigt alternative Datenströme der Datei an.
  /S          Listet Dateien und alle Unterverzeichnisse auf.
  /T          Bestimmt welche Zeit verwendet wird (nur für NTFS).
  Zeit         C  Erstellung
               A  Letzter Zugriff
               W  Letzter Schreibzugriff
  /W          Verwendet Breitformat für die Auflistung.
  /X          Zeigt die Kurznamen für Dateien mit Nicht-8Punkt3-Namen an.
              Das Format ist das gleiche wie bei /N, wobei der Kurzname vor
              dem Langnamen eingefügt wird. Wenn kein Kurzname vorhanden ist,
              werden Leerzeichen angezeigt.
  /4          Zeigt das Jahr vierstellig an.

Optionen können in der Umgebungsvariablen DIRCMD voreingestellt werden.
"-" vor einer Option setzt die Voreinstellung außer Kraft, z. B. DIR /-W.

C:\Users>
```

Abb. 15.8: Mit `dir /?` angezeigte Schalter dieses Befehls

Der Befehl ls

Der Befehl `ls` ist, wie die meisten UNIX-Befehle, sehr leistungsfähig und kennt mehr als 50 verschiedene Schalter. Fürs Erste sehen wir uns nur einen der wichtigeren an, nämlich `-l`.

Die Verwendung von `ls` mit dem Schalter `-l` (der für *long listing* steht, also lange Ausgabe), liefert ausführliche Informationen über Dateien:

```
$ ls -l
-rw-rw-r-- 0 mike 2313443 Jun 13 15:27 bambi.jpg
```

Wir werden uns diese Ausgabe später noch genauer ansehen.

Die Hilfe zu den Befehlen ist in Windows manchmal etwas kryptisch, und auch die in macOS oder Linux mit dem `man`-Befehl angezeigten Beschreibungen können äußerst schwer verständlich sein. Dennoch sind sie sehr nützlich, wenn Ihnen ein Befehl nicht vertraut ist oder Sie nicht herausbekommen können, wie Sie einen Befehl dazu bewegen, das zu tun, was Sie möchten. Ich habe mir eine ganze Reihe von Befehlen gemerkt, rufe die Hilfeseite aber dennoch regelmäßig auf. Das sollten Sie

auch tun. Geben Sie in der Eingabeaufforderung einfach `help` ein, um eine Liste der möglichen Befehle anzuzeigen, wenn Sie nicht weiterkommen.

15.1.11 Arbeitsverzeichnis ändern: Der Befehl cd

Der Befehl `cd` funktioniert in allen Betriebssystemen, es gibt jedoch Unterschiede zwischen Windows, macOS und Linux. Mit dem `cd`-Befehl können Sie in ein anderes Arbeitsverzeichnis wechseln. Sie verwenden den Befehl, indem Sie `cd` gefolgt vom Namen des zu aktivierenden Verzeichnisses eingeben. Um z.B. in Windows zum Verzeichnis `Obiwan` im Hauptverzeichnis zu wechseln, geben Sie `cd \obiwan` ein und drücken ↵. Wenn es das entsprechende Verzeichnis gibt, dann wird das Verzeichnis gewechselt und es wird `C:\Obiwan>` als Eingabeaufforderung angezeigt. Falls es das Verzeichnis `Obiwan` nicht gibt, oder falls Sie sich vertippt und versehentlich `Obiwam` eingegeben haben sollten, dann wird eine Fehlermeldung angezeigt, die auf ein ungültiges Verzeichnis hinweist (»Das System kann den angegebenen Pfad nicht finden«). Ich wünschte, ich hätte bei jeder Anzeige dieser Fehlermeldung einen Euro bekommen! Meistens erhalte ich diese Meldung, wenn ich zu hastig getippt habe. Überprüfen Sie Ihre Eingabe und geben Sie den Befehl erneut ein, falls Ihnen diese Fehlermeldung angezeigt wird.

Hinweis: Fehlermeldungen sind eine feine Sache

Lassen Sie uns einen Moment über Fehlermeldungen nachdenken – nicht nur solche auf der Kommandozeile, wie »Ungültiges Verzeichnis«, sondern auch andere Fehler, die in der grafischen Benutzeroberfläche angezeigt werden. Machen Sie sich wegen Fehlermeldungen keine Sorgen – sie sind eine feine Sache und werden oft stiefmütterlich behandelt, obwohl sie wirklich hilfreich sind.

Überlegen Sie doch einmal, für welche Verwirrung es führen würde, wenn der Computer sich nicht beschweren würde, wenn Sie etwas durcheinanderbringen. Durch Fehlermeldungen erfahren Sie, was Sie falsch gemacht haben, und können das Problem beheben. Sie können keinen Schaden am PC anrichten, wenn Sie den Befehl `dir` oder `cd` nicht richtig eingeben. Nutzen Sie das zu Ihrem Vorteil und machen Sie absichtlich Fehler, um die Fehlermeldungen kennenzulernen. Machen Sie sich einen Spaß daraus, aus Fehlern zu lernen!

Zur Rückkehr zum Stammverzeichnis geben Sie nur `cd \` ein und drücken ↵. Den `cd`-Befehl verwenden Sie, um ein beliebiges Verzeichnis zu aktivieren. Wenn Sie z.B. `cd \franz\backup\test` eingeben, ändert sich auch die Eingabeaufforderung und zeigt `C:\franz\backup\test>` an, allerdings natürlich nur dann, wenn dieses Verzeichnis wirklich existiert.

Wenn sich die Eingabeaufforderung geändert hat, geben Sie erneut `dir` ein. Nun sollte eine Liste mit anderen Datei- und Verzeichnisnamen angezeigt werden. Da alle Verzeichnisse jeweils andere Dateien und Unterverzeichnisse enthalten, zeigt der Befehl `dir` nach Aktivierung eines anderen Verzeichnisses naturgemäß auch andere Daten an.

Das Ändern des Arbeitsverzeichnisses in macOS und Linux funktioniert auf dieselbe Weise, Sie müssen lediglich statt \ ein / verwenden. Sie würden also `cd /Obiwan` oder `cd /franz/backup/test` eingeben, um beim obigen Beispiel zu bleiben.

Hinweis

Auf einem Linux-System Ordner oder Dateien im Stammverzeichnis (/) anzulegen, wird als unhöflich betrachtet. Tatsächlich sind dazu auch root-Rechte erforderlich. Das liegt daran, dass Linux schon immer ein Betriebssystem für mehrere Benutzer war. Daher muss es Einschränkungen geben, damit einzelne Benutzer nicht die Struktur des Betriebssystems durcheinanderbringen können, auf das alle anderen Benutzer angewiesen sind.

In den vorangehenden Beispielen haben wir stets *absolute Pfade* benutzt, also immer den gesamten Pfad des neuen Arbeitsverzeichnisses angegeben. Für alte DOS-Systeme aus den 1980ern war das vielleicht passend, aber bei den heutigen, tief verschachtelten Dateisystemen macht das viel zu viel Arbeit.

Hier kommen *relative Pfade* ins Spiel. Anstatt am Anfang des Pfadnamens immer ein »\« einzugeben, wird nur noch der Name des Ordners angegeben. So könnten Sie beispielsweise vom Stammverzeichnis aus durch Eingabe von `cd Obiwan` in das Verzeichnis `C:\Obiwan` wechseln. Auf diese Weise können Sie mit dem Befehl `cd` schrittweise jeweils eine Verzeichnisebene nach unten wechseln:

```
C:\>cd franz
C:\franz\>cd backup
C:\franz\backup>cd test
```

Oder Sie überspringen mehrere Verzeichnisebenen wie folgt in einem Schritt:

```
C:\>cd franz\backup\test
C:\franz\backup\test>
```

Das funktioniert in macOS und Linux genauso, nur dass Sie natürlich statt des »\« den normalen Schrägstrich »/« eingeben müssen:

```
mike@server:~$ cd Obiwan
mike@server:~/Obiwan$
```

Ein abschließender Trick: Wenn Sie eine Verzeichnisebene nach oben wechseln wollen, dann können Sie dazu `cd` mit zwei anschließenden Punkten eingeben. So können Sie z.B. vom Verzeichnis `C:\franz\backup` in das Verzeichnis `C:\franz` wechseln, wenn Sie einfach `cd ..` eintippen:

```
C:\franz\backup>cd ..
C:\franz>
```

Nehmen Sie sich ein wenig Zeit, um mit dem Befehl `cd` in die verschiedenen Verzeichnisse und Unterverzeichnisse auf Ihrem PC zu wechseln und sich mit `dir` die Inhalte anzeigen zu lassen. Mit `dir` können Sie ein bestimmtes Verzeichnis suchen und mit `cd` dann in dieses Verzeichnis wechseln. Denken Sie daran, dass Sie die Eingabe von `cd \` (bzw. `cd /` in macOS und Linux) immer zum Stammverzeichnis zurückbringt.

Wichtig

Rechnen Sie damit, dass die Option bzw. der Schalter »..« für `dir`, `cd` und andere Befehle in der CompTIA A+-Zertifizierungsprüfung vorkommen. Bei der Navigation mit der Kommandozeile aktiviert er den übergeordneten Ordner.

15.1.12 Laufwerke wechseln

Windows und macOS bzw. Linux verwenden sehr verschiedene Verfahren zum Wechseln von Laufwerken, weil Windows Laufwerksbuchstaben verwendet, die es in macOS und Linux nicht gibt. Wir sehen uns die Funktionsweise erst unter Windows und anschließend in macOS und Linux an.

Laufwerke wechseln unter Windows

Der Befehl `cd` kann *nicht* zum Wechseln von Laufwerken verwendet werden. Um an der Eingabeaufforderung das Laufwerk zu wechseln, brauchen Sie nur den Laufwerksbuchstaben und einen Doppelpunkt einzutippen. Falls z.B. das Verzeichnis `C:\Users\mike` aktiv ist und Sie wollen sich über den Inhalt des USB-Sticks (`E:`) informieren, dann geben Sie nur `e:` ein. Auf dem Bildschirm sieht dies so aus:

```
C:\Users\mike>e:
E:\>
```

Um wieder zum Laufwerk C: zurückzukehren, geben Sie einfach `c:` ein:

```
E:\>c:
C:\Users\mike>
```

Beachten Sie hier, dass Sie sich wieder in demjenigen Verzeichnis befinden, dass Sie zuvor verlassen haben. Geben Sie spaßeshalber doch mal den Laufwerksbuchstaben für ein Laufwerk ein, das es nicht gibt. Mein System besitzt z.B. kein Laufwerk `W:`. Versuche ich, dorthin zu wechseln, erhalte ich folgende Fehlermeldung:

```
Das System kann das angegebene Laufwerk nicht finden.
```

Legen Sie ein optisches Medium ein oder schließen Sie einen RAM-Stick an und versuchen Sie, dorthin zu navigieren. Zeigen Sie mit `dir` den Inhalt des optischen Laufwerks an und ändern Sie mit `cd` das Arbeitsverzeichnis. Kehren Sie abschließend wieder zum Laufwerk `C:` zurück.

Mithilfe der Befehle `dir` und `cd` sowie der Eingabe der Laufwerksbuchstaben können Sie auf sämtliche Ordner aller Speichergeräte Ihres Systems zugreifen. Vergewissern Sie sich, dass Sie mit diesen Befehlen bequem auf Ihrem Computer navigieren können.

Laufwerke wechseln in macOS und Linux

Wenn es in macOS und Linux keine Laufwerksbuchstaben gibt, wie greift man dann auf optische Laufwerke, USB-Sticks und dergleichen zu? Nun, alle Speichergeräte werden als Ordner bereitgestellt, allerdings hängt der Ort dieser Ordner vom Betriebssystem ab. In macOS finden Sie die Geräte im Ordner `/Volumes`. In Ubuntu finden Sie Laufwerke im Verzeichnis `/mnt` und Wechselmedien im Ordner `/media/<Benutzername>`. In anderen Linux-Distributionen müssen Sie sich wohl oder übel selbst auf die Suche begeben. Nur gut, dass Ihnen die Befehle `cd` und `ls` zur Verfügung stehen, oder? Das folgende Kommando zeigt das optische Laufwerk und einen an mein Ubuntu-System angeschlossenen USB-Stick an:

```
mike@server:/media/mike$ ls -l
drwx------ 3 mike mike 4096 Dec 31  1969 USB-STICK
dr-xr-xr-x 6 mike mike 2048 May 13 10:15 Age of Empires
mike@server:/media/mike$
```

15.1.13 Verzeichnisse erstellen

Bis hierhin haben Sie erfahren, wie Sie über die Kommandozeile im System navigieren können. Nun sollten Sie damit beginnen, ein neues Verzeichnis zu erstellen.

Zum Erstellen eines Verzeichnisses verwenden Sie in Windows den Befehl `md` (*make directory*). Alternativ können Sie auch den Befehl `mkdir` nutzen, der in allen Betriebssystemen funktioniert. Um beispielsweise unter Windows einen Ordner namens `Lernen` in Ihrem Benutzerordner zu erstellen,

öffnen Sie ein neues Eingabeaufforderungsfenster oder navigieren mit `cd` zu Ihrem Benutzerordner. Jedenfalls sollte eine Eingabeaufforderung wie diese angezeigt werden:

```
C:Users\mike>_
```

Das Arbeitsverzeichnis ist also das Benutzerverzeichnis des Benutzers »mike«. Geben Sie nun den Befehl zum Erstellen des Verzeichnisses ein:

```
C:\Users\mike>md Lernen
```

Nachdem Sie ↵ gedrückt haben, führt Windows den Befehl aus, gibt aber keine Rückmeldung darüber, was gerade geschehen ist. Um zu überprüfen, ob tatsächlich ein neuer Ordner erstellt wurde, müssen Sie den Befehl `dir` aufrufen:

```
C:\Users\mike>dir
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: 92AC-B31E

 Verzeichnis von C:\Users\mike

04.02.2016  18:47    <DIR>          .
04.02.2016  18:47    <DIR>          ..
21.01.2016  18:30    <DIR>          Contacts
04.02.2016  10:53    <DIR>          Desktop
31.01.2016  16:08    <DIR>          Documents
01.02.2016  11:40    <DIR>          Downloads
21.01.2016  18:30    <DIR>          Favorites
04.02.2016  18:47    <DIR>          Lernen
21.01.2016  18:30    <DIR>          Links
28.01.2016  18:52    <DIR>          Music
04.02.2016  14:44    <DIR>          Pictures
21.01.2016  18:30    <DIR>          Saved Games
21.01.2016  18:30    <DIR>          Searches
21.01.2016  18:30    <DIR>          Videos
     0 Datei(en),              0 Bytes
    14 Verzeichnis(se), 119.895.924.736 Bytes frei

C:\Users\mike
```

Beachten Sie, dass der neue Ordner nicht am Ende der Liste angezeigt wird, wie Sie vielleicht erwartet hätten, die Liste ist nämlich alphabetisch sortiert.

Und was ist mit der Unterscheidung zwischen Groß- und Kleinbuchstaben? Windows zeigt bei Datei- und Ordnernamen zwar beides an, interpretiert Befehle aber so, als ob Sie nur Großbuchstaben verwendet hätten. Benutzen Sie nun den Befehl `md`, um einen Ordner namens `LERNEN` anzulegen (beachten Sie die Großschreibung) und sehen Sie, was passiert. Dasselbe passiert auch unter der grafischen Benutzeroberfläche von Windows. Wechseln Sie zum Desktop und versuchen Sie, zwei Ordner mit den Namen `DATEIEN` und `dateien` anzulegen und sehen Sie, was Windows davon hält.

Zum Erstellen des Unterverzeichnisses `DATEIEN` im Verzeichnis `Lernen` wechseln Sie zunächst mit dem Befehl `cd` in das Verzeichnis `Lernen`:

```
C:Users\mike>cd Lernen
C:Users\mike\Lernen>_
```

Anschließend erstellen Sie mit dem Befehl `md` das Verzeichnis `DATEIEN`:

```
md DATEIEN
```

Hinweis

Vergewissern Sie sich, dass die Eingabeaufforderung immer auf das Verzeichnis verweist, in dem Sie mit dem Befehl `md` das neue Unterverzeichnis anlegen wollen, bevor Sie ihn ausführen.

Geben Sie nach der Ausführung des Befehls `dir` ein, um sich davon zu überzeugen, dass das neue Unterverzeichnis `DATEIEN` tatsächlich angelegt worden ist. Wiederholen Sie die Schritte und legen Sie zum Üben noch das Verzeichnis `Spiele` an. Mit `dir` überprüfen Sie wieder das Ergebnis.

Das Erstellen von Verzeichnissen in macOS und Linux funktioniert wieder auf dieselbe Weise, Sie müssen jedoch statt `md` den Befehl `mkdir` verwenden. Das genannte Beispiel sieht auf meinem Ubuntu-System so aus:

```
mike@server:~$ mkdir Lernen
```

Das Ergebnis kann mit dem Befehl `ls` angezeigt werden:

```
mike@server:~$ ls
Lernen
```

Denken Sie daran, dass Linux Groß- und Kleinschreibung unterscheidet, wie Sie an diesen drei Ordnern sehen können:

```
mike@server:~/Lernen$ ls
dateien  Dateien  DATEIEN
mike@server:~/Lernen$
```

15.1.14 Verzeichnisse löschen

Das Vorgehen beim Löschen von Verzeichnissen entspricht dem beim Erstellen. Wechseln Sie als Erstes in das Verzeichnis mit dem Unterverzeichnis, das Sie löschen möchten. Geben Sie dann den Befehl `rd` (bzw. `rmdir`) (*remove directory*) ein. Beide Befehle funktionieren auf dieselbe Weise. Den Befehl `rmdir` können Sie sowohl unter Windows als auch in macOS und Linux verwenden, den Befehl `rd` hingegen nur unter Windows.

Löschen Sie z.B. in Linux das Unterverzeichnis `DATEIEN` im Verzeichnis `~\Lernen`. (Wie Sie wissen, steht die Tilde für Ihr Benutzerverzeichnis). Wechseln Sie dazu zunächst in das Verzeichnis, in dem sich der Ordner `DATEIEN` befindet (`~\Lernen`), indem Sie den Befehl `cd Lernen` eingeben, nachdem Sie sich vergewissert haben, dass Sie sich in Ihrem Benutzerverzeichnis befinden. Tippen Sie dann `rmdir DATEIEN` ein. Wenn Sie keine Rückmeldung erhalten, konnte der Befehl wahrscheinlich richtig ausgeführt werden! Geben Sie `ls` ein, um zu sehen, ob das Verzeichnis `DATEIEN` gelöscht wurde. In Windows funktioniert das genauso, allerdings verwendet man hier eher den Befehl `rd`, weil er schlicht und einfach kürzer ist.

Der Befehl `rd/rmdir` allein kann keine Verzeichnisse löschen, die noch Dateien oder Unterverzeichnisse enthalten. Wenn Sie ein solches Verzeichnis löschen wollen, müssen Sie zuerst mit dem Befehl `del` (delete) alle Dateien und mit `rd` alle Unterverzeichnisse darin löschen. Unter Windows können Sie zu diesem Zweck aber den Befehl `rd` mit nachgestelltem Schalter `/s` verwenden. `rd /s` löscht Verzeichnisse und alle darin enthaltenen Dateien und Unterverzeichnisse. Der Befehl ist zwar praktisch,

aber auch gefährlich, weil unter Umständen mehr als gewünscht gelöscht wird. Beim Löschen auf der Kommandozeile gibt es keinen Papierkorb, folgen Sie daher immer dem Grundsatz: »Zweimal hinschauen, einmal löschen!«

Löschen Sie als Nächstes die Verzeichnisse `Lernen` und `Spiele` mit `rd /s`. Da sich das Verzeichnis `Lernen` im Stammverzeichnis befindet, wechseln Sie durch Eingabe von `cd \Users\<Benutzername>` zuerst in Ihr Benutzerverzeichnis. Nun führen Sie den Befehl `rd Lernen /s`. In einem seltenen Anfall von Mitleid reagiert Windows darauf so:

```
C:\Users\mike>rd Lernen /s
Möchten Sie "Lernen" löschen (J/N)?
```

Betätigen Sie [J], damit die beiden Verzeichnisse `C:\Users\mike\Lernen` und `C:\Users\mike\Lernen\Spiele` gelöscht werden.

Sie möchten einen Ordner und dessen Inhalt in Linux löschen? Kein Problem, aber dazu verwendet man nicht `rmdir`, sondern den äußerst praktischen Befehl `rm`. (Mehr über `rm` in Abschnitt 15.2.2, *Dateien löschen*.) Im eben geschilderten Fall würde man den Befehl `rm` wie folgt mit dem Schalter `-r` verwenden:

```
mike@server:~$ rm -r Lernen
```

Tipp: Mit Verzeichnissen arbeiten

Als PC-Techniker sollten Sie eine gewisse Übung beim Umgang mit Verzeichnissen haben. Probieren Sie Folgendes aus:

1. Legen Sie in Ihrem Benutzerverzeichnis mit `md` ein neues Verzeichnis `Jedi` an. Tippen Sie dazu in Ihrem Benutzerverzeichnis `md Jedi` ein.
2. Wie gewohnt erhalten Sie keine Rückmeldung, sondern nur eine neue Eingabeaufforderung. Zeigen Sie mit `dir` den Verzeichnisinhalt an, um den neuen Ordner anzuzeigen. Windows legt neue Ordner stets in dem Verzeichnis an, in dem Sie sich gerade befinden, ob Sie das nun beabsichtigen oder nicht. Wechseln Sie durch Eingabe von `cd Jedi` in das neue Verzeichnis.
3. Verwenden Sie den Befehl `md` erneut, um ein Verzeichnis namens `Yoda` anzulegen: `md Yoda`. Lassen Sie sich mit `dir` das neu angelegte Verzeichnis anzeigen.
4. Wechseln Sie mit `cd ..` in das übergeordnete Verzeichnis (Ihr Benutzerverzeichnis), um die angelegten Verzeichnisse mit dem Befehl `rd /s Jedi` zu löschen. Wieder fragt Windows nach, ob Sie die Dateien löschen möchten.
5. Betätigen Sie [J], um die Ordner `Jedi` und `Jedi\Yoda` zu löschen.
6. Wiederholen Sie diesen Vorgang in macOS oder in Linux mit den Befehlen `mkdir`, `cd` und `rm`.

Wichtig

Für die CompTIA A+-Prüfungen sollten Sie die Befehle `md`, `mkdir`, `rd`, `rmdir`, `rm` und `cd` auf jeden Fall beherrschen.

15.1.15 Programme starten in Windows

Zum Start eines Programms über die Eingabeaufforderung wechseln Sie in das Verzeichnis, in dem sich das Programm befindet, geben dann dessen Namen ein und drücken [↵]. Navigieren Sie zum Ordner `C:\Windows\System32`. Geben Sie `dir /p` ein, um sich die Dateien seitenweise anzeigen zu lassen. Darunter müsste sich u.a. eine Datei namens `mmc.exe` befinden (Abbildung 15.9).

```
Eingabeaufforderung - dir /p
29.10.2014  02:58            18.944 midimap.dll
29.10.2014  02:49           237.568 migflt.dll
22.02.2014  11:09            97.280 migisol.dll
21.01.2016  17:05    <DIR>          migration
29.10.2014  03:00           182.784 miguiresource.dll
21.01.2016  17:05    <DIR>          migwiz
22.08.2013  00:48             1.170 migwiz.lnk
29.10.2014  02:31            33.792 mimefilt.dll
29.10.2014  02:03           120.832 mimofcodec.dll
29.10.2014  02:03            32.768 MirrorDrvCompat.dll
29.10.2014  01:53         1.063.424 mispace.dll
29.10.2014  01:59           188.928 miutils.dll
18.06.2013  13:22           673.088 mlang.dat
29.10.2014  01:57           192.512 mlang.dll
29.10.2014  02:37         1.563.136 mmc.exe
29.10.2014  02:48           311.296 mmcbase.dll
29.10.2014  02:46            65.024 mmci.dll
29.10.2014  02:57            11.264 mmcico.dll
29.10.2014  02:24         2.364.928 mmcndmgr.dll
29.10.2014  02:54           114.688 mmcshext.dll
29.10.2014  02:01            74.752 mmcss.dll
29.10.2014  04:07           331.048 MMDevAPI.dll
22.08.2013  05:16         9.576.960 mmres.dll
29.10.2014  02:27           763.392 mmsys.cpl
22.08.2013  02:42             8.960 MMSYSTEM.DLL
Drücken Sie eine beliebige Taste . . .
```

Abb. 15.9: Das Programm `mmc.exe` im Ordner `System32`

Bei allen Dateien mit der Endung `exe` und `com` handelt es sich um Programmdateien, `mmc.exe` ist also ein Programm. Zum Start von `mmc.exe` tippen Sie dessen Namen `mmc` ein und betätigen [↵] (Abbildung 15.10). Beachten Sie, dass Sie dazu die Erweiterung `.exe` nicht eingeben müssen. Damit haben Sie Ihr erstes Programm über die Eingabeaufforderung gestartet!

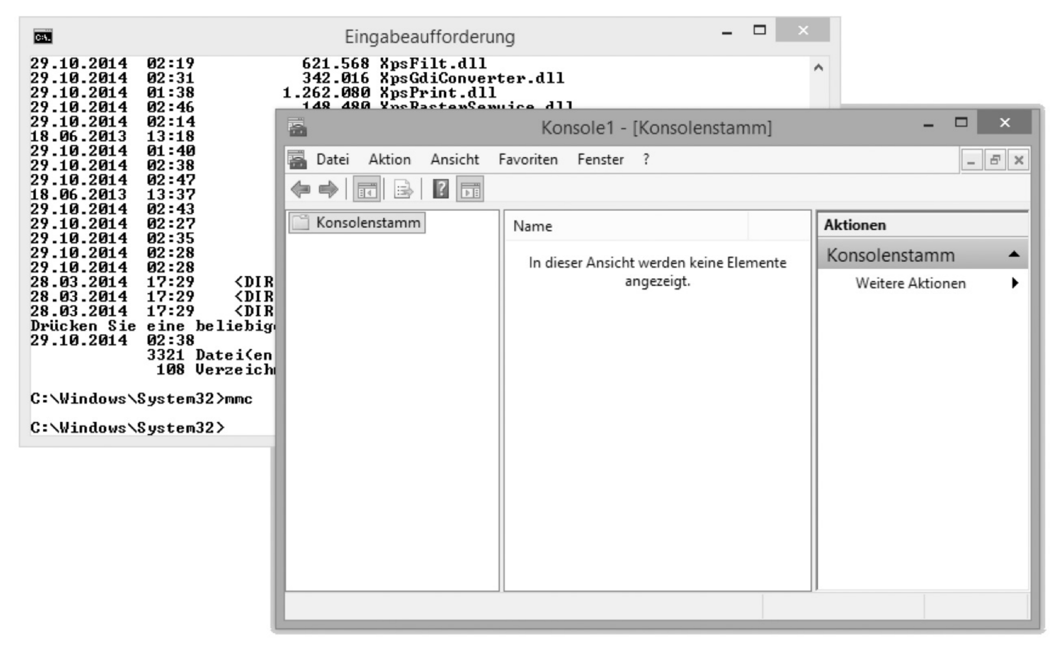


Abb. 15.10: Ausführen von `mmc.exe`

Hinweis

Windows beinhaltet zahlreiche Befehlszeilenwerkzeuge für spezielle Aufgaben, wie beispielsweise das Starten und Beenden von Diensten, die Anzeige von Computern in einem Netzwerk, die Umwandlung von Festplattendateisystemen und vieles andere mehr. Dieses Buch beschreibt die aufgabenspezifischen Werkzeuge in den Kapiteln, die den einzelnen Aufgaben zuzuordnen sind. Beispielsweise enthält Kapitel 19, *Lokale Netzwerke*, eine detaillierte Beschreibung des vielseitigen und leistungsfähigen `net`-Befehls.

15.1.16 Programme starten in macOS und Linux

Ich erzähle den Leuten nur allzu gerne, wie ähnlich sich die Kommandozeilen von Windows, macOS und Linux sind, aber in einigen Bereichen gibt es deutliche Unterschiede. Einer davon ist die Art und Weise, wie man ausführbare Programme von der Kommandozeile aus startet. Ausführbare Programme müssen in macOS oder Linux keine Dateinamenerweiterung wie `.exe` besitzen. Jede beliebige Datei, sei es nun kompilierter Code oder eine Textdatei, kann als ausführbar gekennzeichnet werden (Abbildung 15.11).

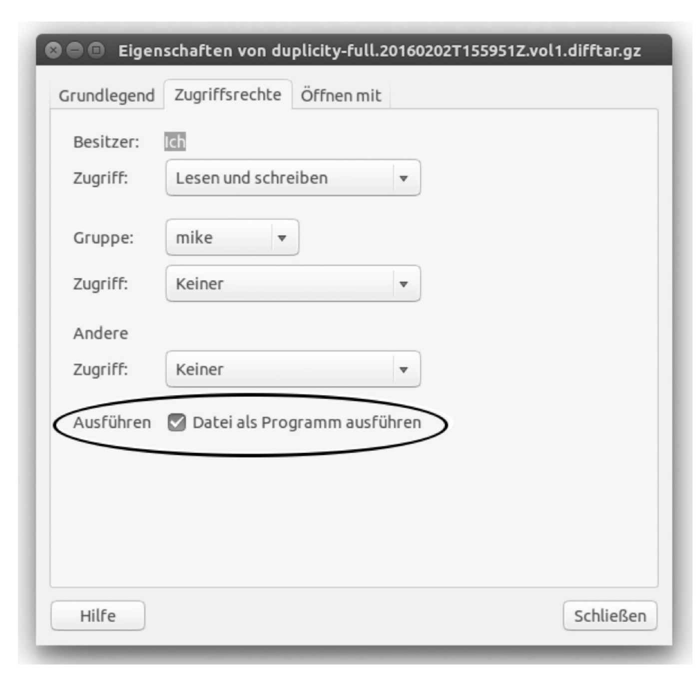


Abb. 15.11: Anzeige der Dateieigenschaften in Ubuntu

Letzten Endes bleibt es also jedem Benutzer selbst überlassen, zu überprüfen, ob er es mit einem Programm zu tun hat. In macOS und Linux startet man nicht planlos irgendwelche Programme, sondern legt Wert darauf zu wissen, worum es sich bei einer Datei handelt, bevor man sie ausführt.

Ausführbare Dateien sind im Terminal von macOS und Linux erkennbar, da bei der Anzeige, wie in Abbildung 15.12, eine Farbcodierung verwendet werden kann (die Sie in der schwarz-weißen Abbildung natürlich kaum erkennen können). In diesem Fall sind ausführbare Dateien grün dargestellt.

Die in macOS und Linux verfügbaren Shells unterscheiden zwei Arten von ausführbaren Programmen: die sogenannten *Built-ins* (in die Shell eingebaute Programme) und »echte« ausführbare Pro-

gramme. Built-ins sind Programme wie das in Abbildung 15.12 verwendete: Befehle wie `ls`, `mkdir` oder `rm`, die Sie soeben kennengelernt haben, sind fest in die Shell integrierte Programme, die Sie starten, indem Sie einfach die Bezeichnung eintippen, wie Sie es in diesem Kapitel schon vielfach getan haben.

```
mike@mike-Ubuntu: /usr/bin
mike@mike-Ubuntu:/usr/bin$ ls -lh gnome-*
-rwxr-xr-x 1 root root 634K Nov  4  2014 gnome-calculator
lrwxrwxrwx 1 root root    9 Jan 31 21:12 gnome-character-map -> gucharmap
-rwxr-xr-x 1 root root 518K Dez  4  2013 gnome-contacts
-rwxr-xr-x 1 root root  44K Apr 10  2014 gnome-disk-image-mounter
-rwxr-xr-x 1 root root 342K Apr 10  2014 gnome-disks
-rwxr-xr-x 1 root root  23K Sep 28  2012 gnome-file-share-properties
-rwxr-xr-x 1 root root  98K Mai 28  2013 gnome-font-viewer
lrwxrwxrwx 1 root root    4 Jan 31 21:12 gnome-help -> yelp
lrwxrwxrwx 1 root root   15 Jan 31 21:12 gnome-keyring -> gnome-keyring-3
-rwxr-xr-x 1 root root  15K Jan 28  2015 gnome-keyring-3
-rwxr-xr-x 1 root root 923K Jan 28  2015 gnome-keyring-daemon
-rwxr-xr-x 1 root root 1,5K Sep 18  2014 gnome-language-selector
-rwxr-xr-x 1 root root  64K Feb  7  2014 gnome-power-statistics
-rwxr-xr-x 1 root root 134K Apr  9  2014 gnome-screensaver
-rwxr-xr-x 1 root root  15K Apr  9  2014 gnome-screensaver-command
-rwxr-xr-x 1 root root  78K Jan 16  2014 gnome-screenshot
-rwxr-xr-x 1 root root 231K Mär 26  2015 gnome-session
-rwxr-xr-x 1 root root  11K Mär 26  2015 gnome-session-inhibit
-rwxr-xr-x 1 root root  64K Mär 26  2015 gnome-session-properties
-rwxr-xr-x 1 root root  11K Mär 26  2015 gnome-session-quit
-rwxr-xr-x 1 root root 136K Jun 24  2013 gnome-system-log
-rwxr-xr-x 1 root root  255 Apr 13  2013 gnome-system-log-pkexec
```

Abb. 15.12: Farbcodierte Anzeige von Dateien in Ubuntu

Ausführbare Programme sind hingegen – nun ja, eben nicht in die Shell integriert. Wenn Sie im Terminal irgendwo ein Programm heruntergeladen haben (was unter Linux durchaus üblich ist), entkomprimieren Sie es und starten es dann. Allerdings gibt es hier ein Problem: Linux kann das Programm nicht finden, obwohl es sich in Ihrem Arbeitsverzeichnis befindet! Interessanterweise ist das jedoch absichtlich so. Wenn Sie versuchen, ein Programm von der Kommandozeile aus zu starten, durchsucht Linux zunächst einmal eine Reihe vorgegebener Verzeichnisse, die in einer sogenannten Umgebungsvariablen namens `PATH` gespeichert sind (nicht zu verwechseln mit den vorhin erwähnten Pfadnamen). Sie können sich diese Verzeichnisse durch Eingabe von `echo $PATH` anzeigen lassen:

```
mike@server:~/$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/
local/games
```

Wenn Sie die Datei ausführen möchten, müssen Sie dem Dateinamen einen Punkt und einen Schrägstrich voranstellen:

```
mike@server:~/$ ./startemich
```

Hinweis

In macOS ist es eher unüblich, im Terminal Programme herunterzuladen und auszuführen, obwohl dies durchaus möglich ist.

15.2 Arbeiten mit Dateien

Dieser Abschnitt befasst sich mit den grundlegenden Funktionen zur Bearbeitung von Dateien. Sie erfahren, wie Sie Dateien anzeigen, kopieren, verschieben, umbenennen und löschen können. Die Beispiele dieses Abschnitts basieren teilweise auf dem Stammverzeichnis `C:\` mit folgenden Dateien und Verzeichnissen:

```
C:\>dir
 Datenträger in Laufwerk C: ist System
 Volumeseriennummer: 036D-250E

 Verzeichnis von C:\
05.05.2010  15:37             4.342 AILog.txt
05.05.2010  15:40             4.433 aoedoppl.txt
05.05.2010  15:40             8.866 aoeWVlog.txt
03.04.2010  18:39         3.948.672 database
05.05.2010  15:43    <DIR>          Docs
26.03.2010  04:22             4.342 LU4.log
18.04.2010  03:02    <DIR>          NVIDIA
27.01.2010  01:55    <DIR>          PerfLogs
05.05.2010  15:46    <DIR>          Pictures
31.03.2010  16:55    <DIR>          Program Files
18.04.2010  02:57    <DIR>          Program Files (x86)
04.02.2010  11:45    <DIR>          Users
19.04.2010  18:27    <DIR>          Windows
               5 Datei(en),      3.970.655 Bytes
      8 Verzeichnis(se), 37.230.673.920 Bytes frei
```

Da Sie wohl kaum einen Rechner mit diesen Dateien und Verzeichnissen besitzen, sollten Sie die Beispiele auf dem eigenen Rechner nachvollziehen. Mit anderen Worten: Arbeiten Sie mit den Ordnern und Dateien, die sich aktuell auf Ihrem System befinden.

15.2.1 Wildcards (Platzhalterzeichen)

Stellen Sie sich einmal vor, dass in einem Verzeichnis 273 Dateien gespeichert sind. Einige dieser Dateien besitzen die Erweiterung `.docx`, die meisten jedoch nicht. Sie suchen aber nur nach Dateien mit der Erweiterung `.docx`. Wäre es nun nicht praktisch, wenn Sie den Befehl `dir` so eingeben könnten, dass nur Dateien mit der Erweiterung `.docx` angezeigt werden? Das ist möglich, wenn Sie mit *Platzhalterzeichen* (*Wildcards*) arbeiten!

Wildcards sind zwei spezielle Zeichen, nämlich der Stern (*) und das Fragezeichen (?), die überall dort als Ersatz für den Namen oder Teile des Namens verwendet werden können, wo Befehle auf mehrere Dateien gleichzeitig angewendet werden sollen. Wildcards lassen sich in den meisten Befehlen an der Eingabeaufforderung nutzen, die mit Dateinamen arbeiten. Ein gutes Beispiel dafür ist der Befehl `dir`. Bei der Ausführung des Befehls `dir` in der Normalform werden alle Dateien und Ordner eines bestimmten Verzeichnisses angezeigt. Sie können aber auch die Suche durch Hinzufügen eines bestimmten Dateinamens eingrenzen. Wenn Sie z.B. `dir ailog.txt` eingeben und das Stammverzeichnis `C:\` aktiv ist, dann kann das Ergebnis so aussehen:

```
C:\>dir ailog.txt
 Datenträger in Laufwerk C: ist System
 Volumeseriennummer: 036D-250E
```

```
 Verzeichnis von C:\

05.05.2010  15:37             4.342 AILog.txt
               1 Datei(en),          4.342 Bytes
    0 Verzeichnis(se), 37.229.711.360 Bytes frei
```

Wenn Sie nur prüfen wollen, ob eine bestimmte Datei an einem bestimmten Ort existiert, ist dies recht praktisch. Nehmen Sie nun an, dass Sie alle Dateien mit der Erweiterung `.txt` anzeigen lassen wollen. Dann müssen Sie die Wildcard * einsetzen, und zwar so: `dir *.txt`. Ersetzen Sie den unbekannten Teil des Dateinamens durch den Stern (*). Das Ergebnis von `dir *.txt` kann so aussehen:

```
C:\>dir *.txt
 Datenträger in Laufwerk C: ist System
 Volumeseriennummer: 036D-250E

 Verzeichnis von C:\

05.05.2010  15:37             4.342 AILog.txt
05.05.2010  15:40             4.433 aoedoppl.txt
05.05.2010  15:40             8.866 aoeWVlog.txt
               3 Datei(en),         17.641 Bytes
    0 Verzeichnis(se), 37.229.711.360 Bytes frei
```

Während der Stern stellvertretend für alle nachfolgenden Zeichen im Dateinamen oder der Erweiterung steht, sodass z.B. die Befehle `dir` und `dir *.*` identisch sind, ersetzt das Wildcard-Zeichen ? einzelne Zeichen. Es ist z.B. dann praktisch, wenn Sie nach Dateinamen mit einer bestimmten Anzahl von Zeichen suchen. Geben Sie z.B. Folgendes ein, um alle Dateien zu finden, deren Dateinamen maximal fünf Zeichen lang sind, mit A beginnen und die Erweiterung `.txt` besitzen:

```
dir A????.txt
Datenträger in Laufwerk C: ist System
 Volumeseriennummer: 036D-250E

 Verzeichnis von C:\

05.05.2010  15:37             4.342 AILog.txt
               1 Datei(en),          4.342 Bytes
    0 Verzeichnis(se), 37.228.998.656 Bytes frei
```

In macOS und Linux funktionieren Wildcards im Wesentlichen auf dieselbe Weise. Sehen Sie sich das Verzeichnis `/bin` auf einem typischen Linux-System an, das voller Dateien ist, und versuchen Sie, den Befehl `ls` zusammen mit Wildcards einzusetzen. Lassen Sie sich beispielsweise alle Dateien anzeigen, die mit dem Buchstaben s anfangen:

```
mike@mike-Ubuntu:/bin$ ls s* -l
-rwxr-xr-x 1 root root 73352 Feb 13  2014 sed
-rwxr-xr-x 1 root root 36232 Mai 23  2013 setfacl
-rwxr-xr-x 1 root root 39896 Feb 18  2013 setfont
-rwxr-xr-x 1 root root 12052 Jan 29  2014 setupcon
lrwxrwxrwx 1 root root     4 Jan 31 21:11 sh -> dash
lrwxrwxrwx 1 root root     4 Jan 31 21:11 sh.distrib -> dash
-rwxr-xr-x 1 root root 31296 Jan 14  2015 sleep
```

```
-rwxr-xr-x 1 root root 76624 Jul 23  2015 ss
-rwxr-xr-x 1 root root 68256 Jan 14  2015 stty
-rwsr-xr-x 1 root root 36936 Jul 15  2015 su
-rwxr-xr-x 1 root root 27200 Jan 14  2015 sync
```

Bisher haben Sie Wildcards lediglich in Verbindung mit dem `dir`-Befehl kennengelernt. Fast alle Befehle akzeptieren aber Wildcards. Befassen wir uns also mit einigen weiteren Befehlen und deren Verwendung von Wildcards!

Tipp

Sehen Sie sich die vier Übungen zum Thema »Wildcards« im Abschnitt über Kapitel 15 unter `http://totalsem.com/100x` an! Damit sind Sie bestens auf entsprechende Fragen in der CompTIA A+-Zertifizierungsprüfung vorbereitet.

15.2.2 Dateien löschen

Zum Löschen von Dateien verwenden Sie in Windows die Befehle `del` oder `erase`. und in macOS und Linux den Befehl `rm`. Das Löschen von Dateien ist einfach (vielleicht allzu einfach!). Von der grafischen Benutzeroberfläche kennen Sie den Komfort des Papierkorbs, aus dem Sie gelöschte Dateien wieder hervorholen können, ein Luxus, auf den Sie an der Eingabeaufforderung aber verzichten müssen. Hier gibt es keine mit dem Papierkorb vergleichbare Funktion. Wenn eine Datei gelöscht wurde, lässt sie sich nur noch mit speziellen Hilfsprogrammen wiederherstellen. (Eventuell, ich würde nicht darauf wetten.) Auch hier sollten Sie Befehle doppelt prüfen, bevor Sie diese ausführen lassen.

Zum Löschen einer einzelnen Datei geben Sie unter Windows den Befehl `del` gefolgt vom Dateinamen ein. Zum Löschen der Datei `Berichtsentwurf1.txt` tippen Sie daher Folgendes ein:

```
del Berichtsentwurf1.txt
```

In macOS und Linux heißt der entsprechende Befehl `rm`:

```
rm Berichtsentwurf1.txt
```

Die Datei wird gelöscht, auch wenn keine Rückmeldung auf dem Bildschirm angezeigt wird. Verwenden Sie `dir` oder `ls`, um sich davon zu überzeugen, dass die Datei tatsächlich gelöscht wurde.

Wie bei `dir` können Sie auch bei `del` und `rm` Wildcards zum Löschen mehrerer Dateien einsetzen. Um z.B. alle Dateien mit der Erweiterung `.txt` in einem Verzeichnis zu löschen, geben Sie in macOS und Linux Folgendes ein:

```
rm *.txt
```

Sie können die Wildcard an beliebiger Position im Dateinamen platzieren. Zum Löschen aller Dateien in einem Verzeichnis, deren Name mit `config.` beginnt, geben Sie `del config.*` ein. Zum Löschen aller Dateien in einem Verzeichnis verwenden Sie das nicht ungefährliche, aber praktische *.* (Stern-Punkt-Stern):

```
del *.*
```

Dies ist einer der wenigen Befehle an der Eingabeaufforderung, die eine Rückfrage zur Folge haben. Nach der Eingabe von `del *.*` werden Sie mit einer Nachfrage wie »Sind Sie sicher (J/N)« oder

»Möchten Sie ... löschen (J/N)?« konfrontiert, die Sie mit J(a) oder N(ein) beantworten. Wenn Sie mit J betätigen, werden alle Dateien im Verzeichnis gelöscht. Passen Sie bei `*.*` also besonders auf!

Unter Windows dient `del` nur zum Löschen von Dateien, nicht aber von Verzeichnissen. Verwenden Sie zu diesem Zweck `rd`. In macOS und Linux können Sie mit dem Befehl `rm` sowohl Dateien als auch Verzeichnisse löschen. Das folgende Beispiel verwendet den Schalter `-r`, um den Ordner `Jedi` und seinen Inhalt zu löschen:

```
rm -r Jedi
```

Der `rd`-Befehl in Windows besitzt den Schalter `/s`, der sich dann genauso verhält wie der Befehl `rm -r`:

```
rd /s Jedi
```

Es liegt auf der Hand, dass die Verwendung der Befehle `rm` und `rd` mit diesen Schaltern gefährlich ist. Verwenden Sie sie mit Bedacht.

Hinweis

Wenn Sie sich im Internet über Terminalbefehle für macOS oder Linux informiert haben, sind Ihnen womöglich Witze begegnet, in denen das Kommando `sudo rm -rf /` eine Rolle spielt. Es weist den Computer an, *sämtliche Dateien und Ordner* zu löschen! `sudo` bedeutet, dass der Befehl mit root-Rechten ausgeführt wird, `rm` ist der Befehl zum Löschen, der Schalter `-r` steht für rekursiv (der Befehle wird mit den Inhalten aller Ordner und Unterordner ausgeführt), `-f` (force) heißt, dass ein Löschen unter allen Umständen erzwungen wird und der Schrägstrich `/` schließlich verweist auf das Stammverzeichnis.

15.2.3 Dateien kopieren und verschieben

Als PC-Techniker müssen Sie Dateien über die Eingabeaufforderung verschieben und kopieren können. Angesichts der Vielzahl der Optionen ist der Befehl `copy` selbst schon schwierig zu erlernen, insbesondere dann, wenn Sie daran gewöhnt sind, Symbole unter Windows zu verschieben. Die folgenden fünf Schritte machen Sie mit dem Vorgang des Verschiebens und Kopierens von Dateien vertraut. Beachten Sie dabei, dass der einzige Unterschied zwischen einem Kopier- und Verschiebevorgang darin besteht, dass beim Kopieren eine Kopie der Datei an der Quellposition zurückbleibt, während nach dem Verschieben (`move`) immer nur eine Datei vorhanden ist. Wenn Sie `copy` erst einmal beherrschen, kennen Sie auch `move`. In macOS und Linux heißen die Befehle zum Kopieren bzw. Verschieben `cp` respektive `mv`.

copy und move in fünf Schritten

Mit dem folgenden Vorgang, der aus fünf Schritten besteht, erlernen Sie auf einfache Art die Verwendung der Befehle `copy` und `move`. Beachten Sie dabei, dass es viele verschiedene Variationen dieser Schritte geben kann. Sobald Sie mit den Befehlen vertrauter geworden sind, können Sie auch einmal ein `copy /?` oder `move /?` in Windows oder `man cp` bzw. `man mv` in macOS und Linux eintippen und sich über die leistungsfähigen Optionen dieser Befehle informieren. Zunächst sollten Sie aber dieser schrittweisen Vorgehensweise folgen:

1. Wechseln Sie an der Eingabeaufforderung in das Verzeichnis, das die Dateien enthält, die Sie kopieren oder verschieben wollen.
2. Geben Sie `copy` oder `move` (Windows) oder `cp` oder `mv` (macOS und Linux) gefolgt von einem Leerzeichen ein.
3. Geben Sie den/die Dateinamen zum Kopieren bzw. Verschieben (mit oder ohne Wildcards) und ein Leerzeichen ein.

4. Geben Sie den Pfadnamen der neuen Speicherposition der Dateien ein.
5. Betätigen Sie ↵.

Schauen Sie sich einmal das folgende Beispiel unter Windows an, in dem die Datei `Notizen.txt` im Verzeichnis `Jedi` in meinem Benutzerordner benutzt wird. Diese Datei soll nun auf einen USB-Stick (`E:`) kopiert werden:

1. Geben Sie `cd Jedi` ein, um das Verzeichnis `Jedi` zu aktivieren.
2. Geben Sie `copy` gefolgt von einem Leerzeichen ein.
3. Geben Sie `Notizen.txt` und ein Leerzeichen ein.
4. Geben Sie `E:\` ein.
5. Betätigen Sie ↵.

Das vollständige Kommando und die Rückmeldung sehen dann so aus:

```
C:\Users\mike\Jedi>copy Notizen.txt E:\
1 Datei(en) kopiert.
```

Wenn Sie das Laufwerk `E:` aktivieren und `dir` eingeben, finden Sie dort die Datei `Notizen.txt`. Probieren Sie ein weiteres Beispiel aus, dieses Mal in macOS oder Linux. Nehmen Sie an, im Verzeichnis `~/Jedi` befinden sich 100 Dateien, von denen 30 die Erweiterung `.odf` besitzen. Nehmen Sie weiter an, dass Sie diese Dateien ins Verzeichnis `~/Drehbücher/sw2020` verschieben wollen. Führen Sie dazu folgende Schritte aus:

1. Geben Sie `cd Drehbücher/sw2020` ein, um in das Verzeichnis `sw2020` zu wechseln.
2. Geben Sie `mv` gefolgt von einem Leerzeichen ein.
3. Geben Sie `*.odf` und ein Leerzeichen ein.
4. Geben Sie `~/Jedi` ein.
5. Drücken Sie ↵.

macOS und Linux geben beim Verschieben keine Rückmeldung, sofern Sie keine speziellen Schalter verwenden. Mit `ls` können Sie überprüfen, ob alle Dateien verschoben wurden.

15.2.4 Durchforsten der Dateihierarchie

Es gibt des Öfteren Situationen, in denen man einen Ordner nicht komplett mit allen darin enthaltenen Unterordnern und den darin befindlichen Dateien und Unterordnern mit einem einzigen Befehl kopieren oder verschieben möchte, sondern nur bestimmte in dieser Ordnerhierarchie befindliche Dateien. Ich bezeichne das als Durchforsten und hier ist die Kommandozeile der grafischen Benutzeroberfläche deutlich überlegen. Wenn man es richtig anstellt, ist das Durchforsten schneller und Sie können den Vorgang viel genauer steuern.

Die Befehle `copy` und `move` lassen sich nur jeweils für ein Verzeichnis einsetzen und sind daher keine gute Wahl für das Kopieren oder Verschieben von Dateien in verschiedenen Verzeichnissen. Microsoft hat daher das Programm `xcopy` entwickelt, um das Kopieren von Dateien in mehreren Ordnern zu erleichtern. (Beachten Sie, dass es keinen Befehl namens `xmove` gibt.) Wir werfen auch noch einen Blick auf `robocopy`, `cp` und `mv`.

xcopy

Der Befehl `xcopy` arbeitet ähnlich wie `copy`, besitzt aber zusätzliche Schalter, die `xcopy` im Hinblick auf die Arbeit mit mehreren Verzeichnissen besonders leistungsfähig machen. Der Befehl funktioniert

folgendermaßen: Nehmen Sie einmal an, dass es auf dem `C:`-Laufwerk ein Verzeichnis namens `Logs` gibt. Das Verzeichnis `Logs` enthält die drei Unterverzeichnisse `Jan`, `Feb` und `Mar`. Alle diese Verzeichnisse einschließlich des Verzeichnisses `Logs` enthalten etwa 50 Dateien. Falls Sie alle diese Dateien mit einem einzigen Befehl auf das Laufwerk `E:` kopieren wollen, geben Sie den folgenden Befehl ein:

```
xcopy c:\Logs e:\Logs /s
```

Da `xcopy` mit Verzeichnissen arbeitet, brauchen Sie die Dateinamen nicht wie bei `dir` anzugeben, auch wenn `xcopy` Dateinamen und Wildcards akzeptiert. Der meistverwendete Schalter `/s` (*subdirectories*) weist `xcopy` an, alle nicht leeren Unterverzeichnisse ebenfalls zu kopieren. Beim Schalter `/e` (*empty*) werden auch leere Unterverzeichnisse mitkopiert. `xcopy` ist das Werkzeug der Wahl, wenn Verzeichnisbäume kopiert werden sollen.

robocopy

Microsoft führte das Kommando `robocopy` vor vielen Jahren mit Windows-Server-Systemen ein, um es Technikern zu ermöglichen, Dateien und Ordner schneller und effizienter als mit `xcopy` oder `copy` zu verwalten. Das leistungsfähige Kommando ermöglicht es beispielsweise, Dateien und Ordner über das Netzwerk auf einen anderen Computer zu kopieren und dabei auf dem Zielsystem die Verzeichnisstruktur des Originals vollständig zu replizieren *und* dort alle Objekte zu entfernen, die nicht Teil dieser Verzeichnisstruktur sind. Das gelingt mit einem einzigen, einfachen Kommando.

Die `robocopy`-Syntax hat keine Ähnlichkeit mit derjenigen von `xcopy`. Wenn Sie `robocopy` einsetzen möchten, müssen Sie sich ein paar Dinge also erneut einprägen. Die grundlegende Syntax lautet:

```
robocopy [Quelle] [Ziel] [Optionen]
```

Es folgt ein Beispiel, das dieses Kommando in Aktion zeigt und alle Dateien und Unterordner aus dem Verzeichnis `D:\testserver\website` des lokalen Rechners in einen freigegebenen Ordner auf dem entfernten Server `\\liveserver\website` kopiert:

```
robocopy d:\testserver\website \\liveserver\website /mir
```

Der Schalter `/mir` (*mirror*) weist `robocopy` an, den vollständigen Inhalt der Quelle zum Ziel zu kopieren, den Inhalt also zu spiegeln. Das bedeutet, dass `robocopy` auf dem Ziel auch Dateien und Ordner löscht, die im Quellverzeichnis nicht vorhanden sind.

Wenn das alles wäre, was `robocopy` leistet, könnte man schon behaupten, dass es ein leistungsfähiges Werkzeug ist, aber es ist nicht einmal die Spitze des Eisbergs. `robocopy` kann auch verschlüsselte Dateien kopieren und ermöglicht es einem Administrator, Dateien zu kopieren, für die der Administrator selbst keine Zugriffsrechte besitzt. Bei Unterbrechungen des Kopiervorgangs (z.B. durch einen temporären Ausfall des Netzwerks) wird dieser an der Stelle wieder aufgenommen, an der die Unterbrechung stattfand. Die vollständige Syntax können Sie sich durch Eingabe von `robocopy /?` anzeigen lassen.

Die Funktionsvielfalt und Nützlichkeit von `del`, `copy`, `move`, `xcopy` und `robocopy` machen diese Kommandos für PC-Techniker unentbehrlich, aber diese Leistungsfähigkeit birgt auch Gefahren. Hüten Sie sich davor, so nebenbei mal ein paar dieser Kommandos abzusetzen. Überlegen Sie vor der Ausführung eines solchen Kommandos lieber zweimal. Die Daten, die Sie dadurch vielleicht bewahren, könnten Ihre eigenen sein!

Wichtig

Sie sollten sich für die CompTIA A+-Prüfung mit `xcopy` und `robocopy` auskennen.

Nochmals cp und mv

Wenn Sie sich mit wirklich leistungsstarken Befehlen befassen möchten, sollten Sie sich die UNIX-Befehle ansehen. Anders als in Windows können Sie mit denselben Befehlen `cp` und `mv`, die wir zum Kopieren und Verschieben von Dateien verwendet haben, auch Ordner und ihre Inhalte sowohl kopieren als auch verschieben. Betrachten wir den Ordner `/home/mike/Backups`, der zehn Unterordner und Hunderte Dateien enthält. Ich möchte nun eine Kopie dieser Dateien in einem Ordner namens `/mnt/storage` speichern. Zu diesem Zweck muss ich nur den Befehl `cp` mit dem Schalter `-R` (wie rekursiv) ausführen. (Die Tilde in der Eingabeaufforderung weist daraufhin, dass ich mich in meinem Benutzerordner befinde.)

```
mike@server:~$ cp -R Backups /mnt/storage
```

Falls ich die Dateien nicht kopieren, sondern verschieben möchte, verwende ich statt des Befehls `cp` einfach `mv`. Bemerkenswerterweise ist beim `mv`-Befehl noch nicht einmal ein Schalter erforderlich – rufen Sie den Befehl einfach nur mit dem fraglichen Ordner und dem Ziel auf:

```
mike@server:~$ mv Backups /mnt/storage
```

15.3 Ausgewählte Windows-Befehle

Als tüchtiger IT-Techniker im Außeneinsatz müssen Sie mit einer Menge von Befehlszeilenprogrammen und anderen wichtigen Dienstprogrammen vertraut sein. Die Prüfung 220-1002 der CompTIA konzentriert sich nur auf einige dieser Programme. Und obwohl viele bereits in vorherigen Kapiteln detailliert vorgestellt wurden, ist es äußerst wichtig, dass Sie `chkdsk`, `format`, `hostname`, `gpupdate`, `gpresult`, `sfc`, und `shutdown` verstehen und praktisch einsetzen können.

15.3.1 chkdsk (/f /r)

Der Befehl `chkdsk` (*checkdisk*) durchsucht Festplatten und Volumes und kann Fehler und Probleme beheben, die er darauf erkennt. Sie können das Dienstprogramm `chkdsk` von der Befehlszeile aus mit den Schaltern `/f` und `/r` ausführen. Der Schalter `/f` versucht, Fehler auf den Volumes zu beheben, während der Schalter `/r` defekte Sektoren ausfindig zu machen und diese zu reparieren versucht. Um erfolgreich ausgeführt zu werden, benötigt `chkdsk` direkten Zugriff auf ein Laufwerk. Anders ausgedrückt muss das Laufwerk »entsperrt« sein. Wenn Sie `chkdsk /f /r` ausführen und das Laufwerk nicht entsperrt werden kann, dann erhalten Sie die Meldung »Das aktuelle Laufwerk kann nicht gesperrt werden«, was bedeutet, dass ein anderer Prozess das Laufwerk gesperrt hat und damit verhindert, dass `chkdsk` das Laufwerk selbst sperren kann. Danach bietet Ihnen `chkdsk` die Option an, den Befehl beim nächsten Neustart des Systems auszuführen (Abbildung 15.13).

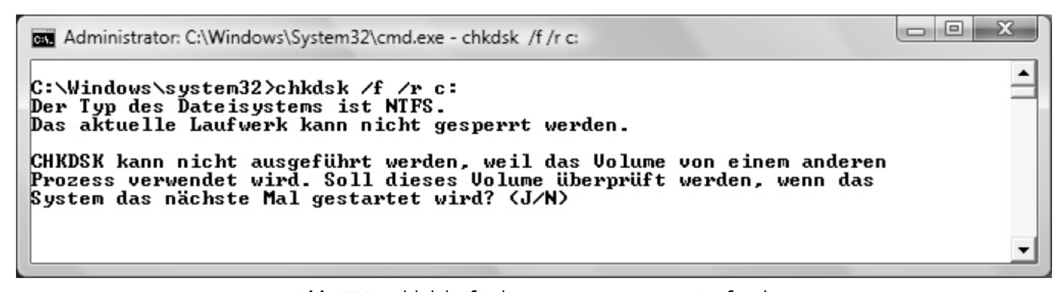


Abb. 15.13: chkdsk /f /r bei einem gesperrten Laufwerk

15.3.2 format

Nach den vorhergehenden Kapiteln sollten Sie eigentlich Experte im Formatieren und Partitionieren von Festplatten sein (oder zumindest ziemlich gut damit vertraut sein). Wie Sie wissen, handelt es sich bei der Formatierung um den Vorgang des Löschens oder der Vorbereitung eines Volumes (oder ehemals Partition) für die Aufnahme eines Betriebssystems oder von Daten. Wir sind bereits die verschiedenen verfügbaren Windows-internen Dienstprogramme durchgegangen, mit denen Laufwerke formatiert werden können, und zweifellos wissen Sie, dass eine Unmenge entsprechender Dienstprogramme von Drittanbietern erhältlich ist. In diesem Kapitel müssen Sie sich nur mit dem Befehl `format` und seinen Schaltern vertraut machen.

Wie Sie sich sicher denken können, werden mit dem Befehl `format` Volumes über die Eingabeaufforderung formatiert. Abbildung 15.14 zeigt ein Beispiel für den `format`-Befehl in Aktion. Beachten Sie die Schalter, mit denen ich angeben kann, welches Dateisystem verwendet werden soll, dass ich Komprimierung wünsche etc. Am besten machen Sie sich mit dem Befehl `format` und seinen verfügbaren Schaltern einfach durch Eingabe von `format /?` an der Eingabeaufforderung vertraut.

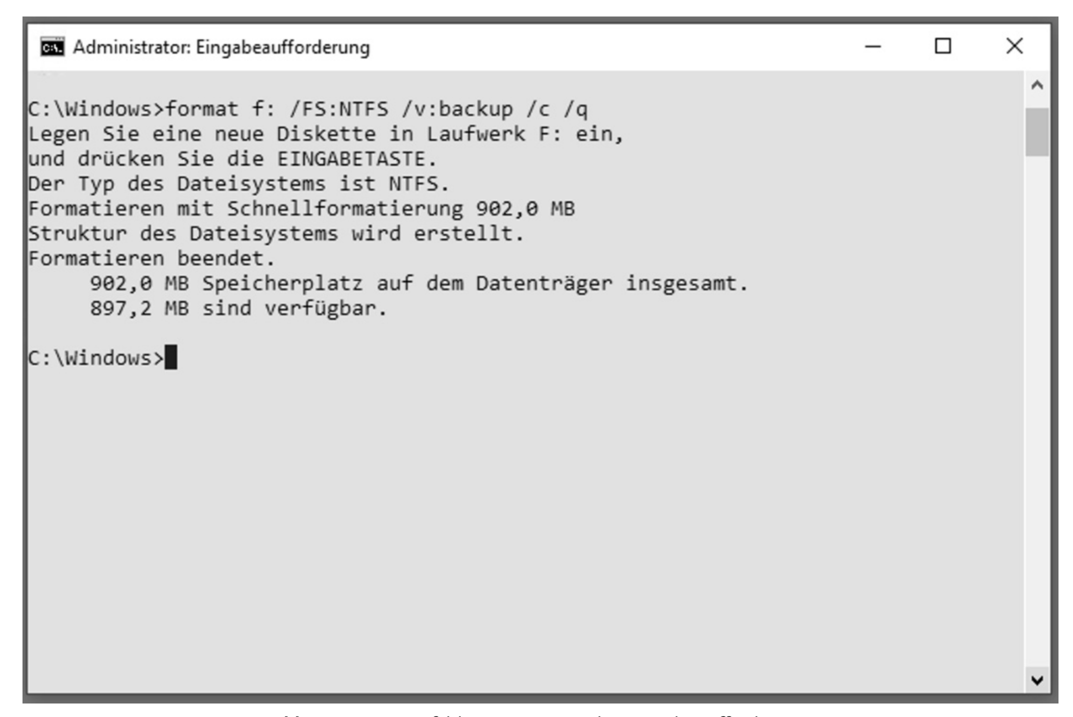


Abb. 15.14: Der Befehl `format /?` in der Eingabeaufforderung

Die A+-Prüfungen der CompTIA berücksichtigen sowohl die unter der grafischen Benutzeroberfläche verfügbaren Dienstprogramme und Optionen als auch die auf der Kommandozeile bereitstehenden Programme, daher sollten Sie sich auch mit dem Befehl `format` und dessen Schaltern vertraut machen und diese auf einem Testsystem ausprobieren, bei dem Sie wirklich bedenkenlos alle Daten löschen können. Abgesehen davon können Sie sich auch nie sicher sein, welche Leichen die CompTIA noch im Keller hat.

15.3.3 hostname

`hostname` ist wohl der geradlinigste aller Kommandozeilenbefehle. Nach der Eingabe von `hostname` wird Ihnen der Name Ihres Computers angezeigt. Bei mir wird beispielsweise »MikesPC« ausgegeben. (Dieser Befehl gehört nicht zu den Lernzielen der CompTIA, aber es ist nützlich, ihn zu kennen.)

15.3.4 gpupdate

Gruppenrichtlinien sind das Fundament der Sicherheitseinstellungen für Windows-Systeme und es gibt buchstäblich Tausende davon. Gruppenrichtlinien legen wichtige Sicherheitsaspekte fest, wie z.B. die Komplexität des Kennworts, die erlaubte Anzahl von Anmeldeversuchen und sogar ob es einem Benutzer gestattet ist, Software zu installieren. Gruppenrichtlinien sind auf eigenständige Computer oder auf Systeme in einer Windows-Domäne anwendbar. Wenn Sie hier Änderungen vornehmen, kann es allerdings eine Weile dauern, bis diese auch in Kraft treten. Wenn Sie möchten, dass die neuen Gruppenrichtlinien unverzüglich wirksam werden, können Sie das Kommandozeilenprogramm `gpupdate` verwenden.

15.3.5 gpresult

Wenn Sie an einem schnellen Überblick über die für einen bestimmten Benutzer oder Computer gültigen Gruppenrichtlinien interessiert sind, ist `gpresult` das richtige Werkzeug. Microsoft bezeichnet es auch als *Gruppenrichtlinienergebnis-Tool*. Sie können `gpresult` für jeden Benutzer oder Computer im Netzwerk ausführen – vorausgesetzt, Sie verfügen über einen gültigen Benutzernamen und das dazugehörige Kennwort. Sie können detaillierte Anfragen stellen oder eine Zusammenfassung abrufen. Der nachstehende Befehl zeigt die Zusammenfassung für den Benutzer `mike meyers` des lokalen Computers (Ausgabe gekürzt):

```
C:\>gpresult /USER "mike meyers" /R

Betriebssystem Microsoft (R) Windows (R) Gruppenrichtlinienergebnis-Tool v2.0
c 2013 Microsoft Corporation. All rights reserved.

Am 05.02.2016 um 17:45:12 erstellt
RSOP-Daten für IE11Win8_1\Mike Meyers auf IE11WIN8_1: Protokollmodus
---------------------------------------------------------------------

Betriebssystemkonfiguration: Eigenständige Arbeitsstation
Betriebssystemversion:       6.3.9600
Standortname:                Nicht zutreffend
Roamingprofil:Nicht zutreffend
Lokales Profil:              C:\Users\mike
Langsame Verbindung?         Nein

BENUTZEREINSTELLUNGEN
----------------------

    Letzte Gruppenrichtlinienanwendung:   05.02.2016, um 15:41:59
    Gruppenrichtlinieanwendung von:       Nicht zutreffend
    Schwellenwert für langsame Verbindung:500 kbps
    Domänenname:                          IE11Win8_1
    Domänentyp:                           <Lokaler Computer>
```

15.3.6 sfc

`sfc` (*System File Checker*), das Windows-Ressourcenüberprüfungsprogramm oder einfach `sfc.exe`, durchsucht das System nach wichtigen Windows-Systemdateien und stellt diese neben wichtigen Ordnern und Pfaden wieder her. Techniker benutzen das `sfc`-Dienstprogramm häufig aus einer noch funktionierenden Windows-Version oder von einer Windows-Installationsdisc aus, um eine beschädigte Windows-Umgebung zu reparieren. Wenn Sie `sfc` ausführen und Probleme erkannt werden, dann versucht das Programm, beschädigte oder fehlende Dateien durch die im Verzeichnis `Windows\System32\Dllcache\` zwischengespeicherten DLLs zu ersetzen. Ohne allzu tief in die damit verbundene Wissenschaft abzutauchen, sollten Sie zumindest wissen, dass Sie `sfc` zur Reparatur beschädigter Systemdateien einsetzen können. Um `sfc` von der Eingabeaufforderung aus zu starten, geben Sie `sfc /scannow` ein. Um sich selbst mit den verschiedenen Schaltern vertraut zu machen, geben Sie `sfc /?` ein (Abbildung 15.15).

```
Administrator: C:\Windows\System32\cmd.exe
C:\>sfc /?

Microsoft(R) Windows XP-Ressourcenüberprüfungsprogramm, Version 6.0
Copyright (C) 2006 Microsoft Corporation. Alle Rechte vorbehalten.

Überprüft alle geschützten Systemdateien und ersetzt falsche Versionen mit
Microsoft-Originalversionen.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>]
    [/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory>
]

/SCANNOW        Überprüft die Integrität aller geschützter Systemdateien und
                repariert ggf. Dateien mit Problemen.
/VERIFYONLY     Überprüft die Integrität aller geschützter Systemdateien.
                Es erfolgt keine Reparatur.
/SCANFILE       Überprüft die Integrität der angegebenen Datei, und
                repariert ggf. die Datei, wenn Probleme gefunden werden.
                Es muss ein vollständiger Pfad angegeben werden. Pfad <Datei>
/VERIFYFILE     Überprüft die Integrität der angegebenen Datei.  Es erfolgt
                keine Reparatur.
/OFFBOOTDIR     Gibt den Speichort des Offlinestartverzeichnisses für
                Offlinereparaturen an.
/OFFWINDIR      Gibt den Speichort des Offline-Windows-Verzeichnisses für
                Offlinereparaturen an.

e.g.

        sfc /SCANNOW
        sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
        sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDI
R=d:\windows
        sfc /VERIFYONLY

C:\>_
```

Abb. 15.15: Anzeige der Optionen des Befehls `sfc`

15.3.7 shutdown

Mit dem Befehl `shutdown` können Sie lokale oder entfernte Computer herunterfahren oder neu starten. Das Interessante an diesem Befehl sind die verschiedenen Schalter, die Sie verwenden können, um das Herunterfahren bzw. den Neustart zu steuern. Beispielsweise könnte ein Netzwerkadministrator ein entferntes System mit wenigen Tastendrücken neu starten:

```
shutdown /r /m \\devserver
```

Der Schalter `/r` weist `shutdown` an, den Computer neu zu starten, statt ihn herunterzufahren. Geben Sie zur Anzeige der vollständigen Syntax den Befehl `shutdown /?` ein.

15.3.8 Verwendung der Funktionstasten in Windows

Falls Sie in der Eingabeaufforderung wiederholt dieselben oder wenigstens einander sehr ähnliche Befehle eingeben müssen, stellt Microsoft eine Reihe von Verfahren zur Verfügung, mit denen Sie auf bereits eingegebene Befehle wiederholt zurückgreifen können. Geben Sie z.B. an der Eingabeaufforderung `dir` ein. Wieder an der Eingabeaufforderung betätigen Sie F1. Nun sehen Sie den Buchstaben »d«. Bei erneuter Betätigung von F1 erscheint nach dem »d« der Buchstabe »i«. Mit F1 können Sie also die einzelnen Buchstaben des vorherigen Befehls einzeln zurückholen. Mit F3 wird der komplette, zuletzt eingegebene Befehl angezeigt. Jetzt probieren Sie die folgenden drei Befehle aus:



```
dir /w
hostname
md Skywalker
```

Drücken Sie jetzt die Taste ↑. Drücken Sie diese so lange, bis Sie Ihren ursprünglichen `dir`-Befehl wieder sehen – Sie sehen den Verlauf für alle Ihre ausgeführten Befehle. Jetzt drücken Sie → und tragen am Ende Ihres `dir`-Befehls `/p` ein. Die Nutzung des Befehlsverlaufs unter Windows ist sehr praktisch.

Hinweis

Für die Shells in macOS und Linux gibt es ebenfalls verschiedene Sondertasten, von denen viele denen in Windows ähneln. Tatsächlich hat Windows viele der praktischen Tastaturkürzel von der UNIX-Welt kopiert. macOS und Linux gehen beim Befehlsverlauf sogar noch einen Schritt weiter und speichern ihn, sodass er erhalten bleibt, selbst wenn Sie das Terminal beenden oder den Rechner neu starten. Das erweist sich als sehr nützlich, wenn Sie Ihr Terminalfenster versehentlich geschlossen haben. Die Shells in macOS und Linux verwenden zwar anders als Windows nicht die Funktionstasten, sondern viele Tastaturkürzel, bei denen die Taste Strg Verwendung findet. Mit der Tastenkombination Strg + R können Sie beispielsweise den Befehlsverlauf durchsuchen. Das ist enorm nützlich, wenn Sie einen wirklich komplizierten Befehl eingegeben haben und zwei Wochen später feststellen, dass Sie ihn erneut benötigen.

15.3.9 PowerShell

Microsofts *PowerShell* ist ein leistungsfähigerer Ersatz für die herkömmliche Windows-Eingabeaufforderung. Die PowerShell kennt die traditionellen Befehle `dir`, `cd`, `md` usw. ebenfalls, bringt aber eine Reihe erheblich leistungsfähigerer Werkzeuge mit, die als *Cmdlets* (sprich: »Commandlets«) bezeichnet werden, mit denen Sie erstaunliche Dinge erledigen können. Abbildung 15.16 zeigt zwei Kommandos, die normalerweise dasselbe tun, nämlich den Inhalt eines Verzeichnisses anzeigen: `dir` und `Get-ChildItem`.

Wie Sie wissen, können Sie mit `dir *.jpg` in einem Verzeichnis beispielsweise nach JPEG-Dateien suchen. Mit der PowerShell können Sie das Ganze auch ein paar Nummern größer bekommen. Das folgende Kommando findet nicht nur alle JPEG-Dateien auf dem gesamten Computer, sondern außerdem noch alle Vorkommen von JPEG-Dateien in Dokumenten (wie etwa Word-, PowerPoint- oder PDF-Dateien):

```
Get-ChildItem . -Include *.jpg -Recurse -Force
```

Falls es Sie interessiert, was die einzelnen Bestandteile dieses Cmdlets bedeuten: `Get-ChildItem` ist der Hauptbefehl. Der Punkt ».« steht für das aktuelle Verzeichnis und alle Unterverzeichnisse. `-Include *.jpg` teilt dem Kommando mit, nach welchem Dateityp gesucht werden soll, der Parameter `-Recurse` sorgt dafür, dass auch die Unterverzeichnisse durchsucht werden, und `-Force` schließlich findet auch versteckte Dateien. Es ist wie ein gedoptes `dir`!

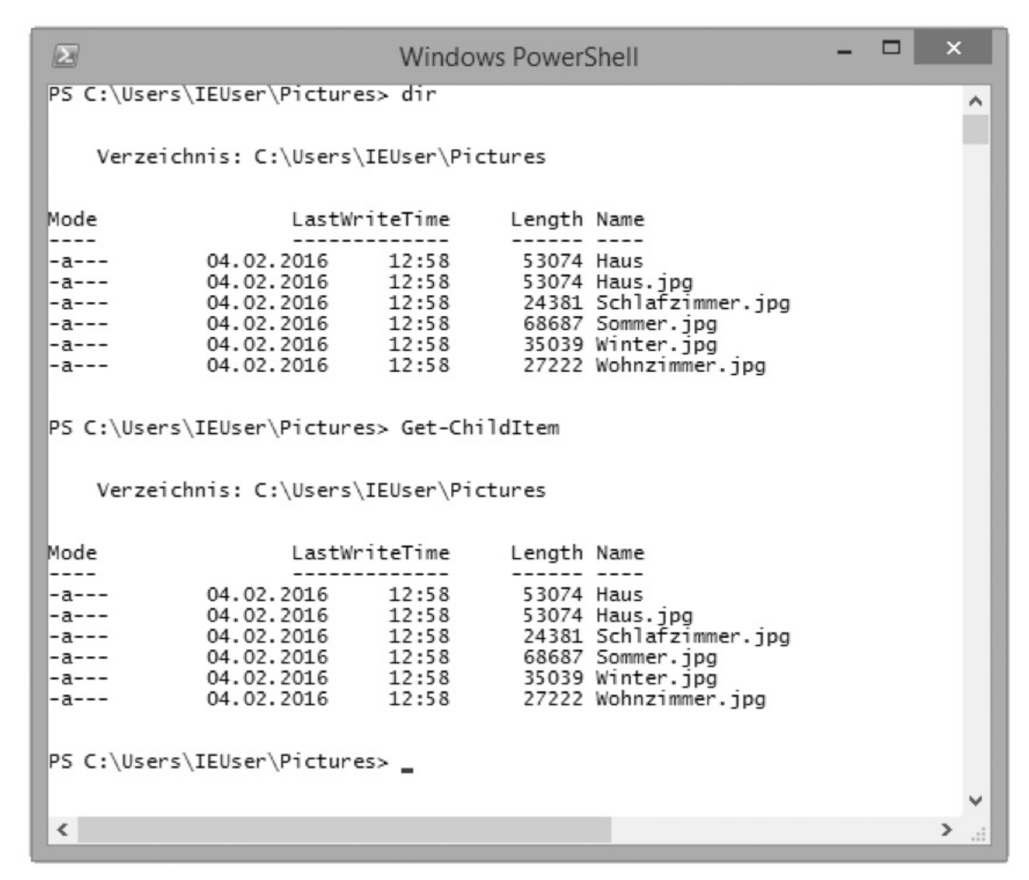


Abb. 15.16: Einfache Befehle in der PowerShell

Damit haben wir nur an der Oberfläche dessen gekratzt, was mit der PowerShell machbar ist. Wenn Sie selbst damit herumexperimentieren möchten, geben Sie einfach PowerShell in das Suchfeld ein und drücken Sie [↵]. Viel Vergnügen!

15.4 Eine Auswahl von Befehlen in macOS und Linux

macOS und Linux bringen eine Vielzahl von Kommandozeilenbefehlen mit und es ist eine Unmenge erstaunlich leistungsfähiger Tools von anderen Entwicklern verfügbar. Eine der interessantesten Herausforderungen bei der Arbeit mit dem Terminal ist die Tatsache, dass es für nahezu alle Aufgaben mehr als ein Werkzeug bereitsteht (mehr dazu in Abschnitt 15.4.6 über den Editor `vi`). An dieser Stelle sehen wir uns die in den Lernzielen der CompTIA A+-Zertifizierungsprüfung erwähnten Kommandos an, denn Sie könnten den Rest Ihres Lebens damit verbringen, alle verfügbaren Terminal-Befehle zu erlernen!

Hinweis

Die ersten beiden vorgestellten Kommandos `ifconfig` und `iwconfig` setzen einige Netzwerkkenntnisse voraus. Wenn Netzwerke für Sie noch Neuland sind, können Sie diesen Abschnitt jetzt überspringen und ihn nach der Lektüre der Kapitel 18 bis 21 lesen.

15.4.1 ifconfig

Der Befehl `ifconfig` ermöglicht es Ihnen, die Einstellungen Ihrer Netzwerkverbindung anzuzeigen und zu ändern. Die Ausführung von `ifconfig` liefert eine Ausgabe wie die unten stehende. Bei Ihnen wird sie zweifelsohne etwas anders aussehen.

```
mike@mike-Ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  Hardware Adresse 08:00:27:7e:29:11
          inet Adresse:10.0.2.15  Bcast:10.0.2.255  Maske:255.255.255.0
          inet6-Adresse: fe80::a00:27ff:fe7e:2911/64
Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
          RX-Pakete:192 Fehler:0 Verloren:0 Überläufe:0 Fenster:0
          TX-Pakete:210 Fehler:0 Verloren:0 Überläufe:0 Träger:0
          Kollisionen:0 Sendewarteschlangenlänge:1000
          RX-Bytes:95304 (95.3 KB)  TX-Bytes:23945 (23.9 KB)

lo        Link encap:Lokale Schleife
          inet Adresse:127.0.0.1  Maske:255.0.0.0
          inet6-Adresse: ::1/128 Gültigkeitsbereich:Maschine
          UP LOOPBACK RUNNING  MTU:65536  Metrik:1
          RX-Pakete:218 Fehler:0 Verloren:0 Überläufe:0 Fenster:0
          TX-Pakete:218 Fehler:0 Verloren:0 Überläufe:0 Träger:0
          Kollisionen:0 Sendewarteschlangenlänge:0
          RX-Bytes:16507 (16.5 KB)  TX-Bytes:16507 (16.5 KB)
```

macOS und Linux verwenden spezielle Bezeichnungen für die verschiedenen Netzwerkanschlüsse:

- `eth0`, `eth1`, `en0`, `en1` usw.: kabelgebundene Ethernet-Netzwerkanschlüsse
- `wlan0`, `wlan1` usw.: drahtlose Netzwerkanschlüsse nach dem Standard IEEE 802.11
- `lo`: Loopback (Netzwerktest)

Sie können einen Netzwerkanschluss wie folgt deaktivieren:

```
mike@mike-Ubuntu:~$ ifconfig eth0 down
```

Hinweis

Nach Maßgabe der CompTIA müssen Sie mit dem Befehl `ifconfig` vertraut sein. In macOS ist er noch in Gebrauch, in Linux gilt er hingegen als veraltet und wird zunehmend durch ein Werkzeug mit dem schlichten Namen `ip` ersetzt, der dasselbe und mehr leistet als `ifconfig`. Geben Sie im Terminal `man ip` ein, wenn Sie mehr darüber erfahren möchten.

Mit `ifconfig` können Sie außerdem vorübergehend die IP-Einstellungen ändern. Der folgende Befehl weist dem drahtlosen Netzwerkanschluss bis zum nächsten Rechnerstart die IP-Adresse 192.168.4.15 zu:

```
mike@mike-Ubuntu:~$ sudo ifconfig wlan0 192.168.4.15
```

Hinweis

In Windows gibt es einen Befehl, der `ifconfig` und `ip` sehr ähnlich ist und `ipconfig` heißt. Hier findet er nur beiläufig Erwähnung, aber in Kapitel 19 wird er seine ganze Leistungsstärke zeigen.

15.4.2 iwconfig

Der Befehl `ifconfig` ist ein leistungsfähiges Werkzeug, aber wenn Sie die Einstellungen des drahtlosen Netzwerks anzeigen oder ändern möchten, benötigen Sie `iwconfig`. Die Eingabe von `iwconfig` (ohne Parameter) liefert diese Ausgabe:

```
mike@mike-Ubuntu:~$ iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11bg  ESSID:"TOTALHQ"  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency:2.452 GHz  Access Point: 00:0F:76:32:FA:E6
          Bit Rate:54 Mb/s   Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=100/100  Signal level=95/100  Noise level=0/100
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

lo        no wireless extensions.
```

Zum Ändern der SSID von `wlan0` auf »NeueSSID« geben Sie Folgendes ein:

```
mike@mike-Ubuntu:~$ sudo iwconfig wlan0 essid "NeueSSID"
```

Beachten Sie, dass `iwconfig` nicht dazu gedacht ist, IP-Informationen anzuzeigen, denn das gehört zu den Aufgaben von `ifconfig`.

15.4.3 ps

Wenn Sie sich die auf Ihrem System aktiven Prozesse ansehen möchten, benötigen Sie den Befehl `ps`. Dieser schon sehr alte Befehl dient zur Anzeige detaillierter und anpassbarer Informationen über die laufenden Prozesse. Wie alt der Befehl ist, zeigt sich auch daran, dass es zwei verschiedene Sätze von Schaltern für ihn gibt! Wie dem auch sei: Sehen wir uns ein Beispiel für die wohl gebräuchlichste Verwendung des Befehls an: den Befehl `ps aux`. Genau genommen handelt es sich dabei um den Befehl `ps` mit den drei Schaltern `a` (= Prozesse aller Benutzer anzeigen), `u` (= Eigentümer der Prozesse anzeigen) und `x` (= nicht einem Terminal zugeordnete Prozesse anzeigen).

```
mike@mike-Ubuntu:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3  33792  4056 ?        Ss   11:24   0:01 /sbin/init
   .
   .
   .
mike      2047  0.0  2.2 583476 22996 ?        Sl   11:26   0:00 update-notifier
mike      2070  0.1 17.9 662976 182228 ?       SNl  11:26   0:02 /usr/bin/python3 /usr/bin/upda
mike      2086  0.0  0.8 469016  8296 ?        Sl   11:27   0:00 /usr/lib/x86_64-linux-gnu/deja
mike      2096  0.0  2.5 681216 25924 ?        Sl   11:29   0:00 /usr/lib/x86_64-linux-gnu/unit
mike      2109  0.0  3.2 597652 33084 ?        Sl   11:29   0:00 /usr/bin/unity-scope-loader ap
mike      2112  0.0  1.4 718672 15036 ?        Sl   11:29   0:00 /usr/lib/x86_64-linux-gnu/unit
mike      2134  0.0  1.4 352172 15024 ?        Sl   11:29   0:00 /usr/lib/x86_64-linux-gnu/unit
mike      2162  0.0  1.3 484164 14232 ?        Sl   11:29   0:00 /usr/lib/gvfs/gvfsd-http --spa
mike      2180  0.0  3.1 550692 32536 ?        Rl   11:29   0:00 gnome-terminal
mike      2187  0.0  0.1  14828  1920 ?        S    11:29   0:00 gnome-pty-helper
mike      2188  0.0  0.5  28468  5376 pts/0    Ss   11:29   0:00 bash
mike      2350  0.0  0.2  24172  2608 pts/0    R+   12:13   0:00 ps aux
mike@mike-Ubuntu:~$
```

Bei der Verwendung des Befehls `ps` bereitet die enorme Größe der Ausgabe die meisten Schwierigkeiten. Es gibt jedoch eine Reihe von Möglichkeiten, dieses Problems Herr zu werden, z.B. die Verwendung von `ps | less`. Das Programm less erleichtert es, in der Ausgabe von `ps` hoch und runter zu scrollen. Erinnern Sie sich an das Programm more, das am Anfang dieses Kapitels erwähnt wurde? Nun, `less` *ist* `more`, um nicht zu sagen: Weniger ist mehr ... Aber im Ernst: Für diese Aufgabe sind `less` und `more` gleich gut geeignet. Die beiden Tools unterscheiden sich nur in Details, die für sehr erfahrene Benutzer oder Programmierer von Interesse sind.

Sehen wir uns die Ausgabe von `ps` genauer an:

- `USER`: Wer führt den Prozess aus?
- `PID`: Die dem Prozess zugewiesene ID.
- `%CPU`: Der Prozentsatz der vom Prozess beanspruchten CPU-Rechenleistung.
- `%MEM`: Der Prozentsatz des vom Prozess belegten Arbeitsspeichers.
- `VSZ`: Ausgelagerter Speicher in Kilobyte.
- `RSS`: Belegter physischer Speicher in Kilobyte.
- `TTY`: Das Terminal, das Ausgaben des Prozesses entgegennimmt.
- `STAT`: S = Warten, R = Arbeitet, l = Multithreaded, + = Vordergrundprozess
- `START`: Startzeitpunkt des Prozesses
- `TIME`: Laufzeit des Prozesses
- `COMMAND`: Der Name des ausführbaren Programms, das den Prozess erzeugt hat.

Häufig benutzt man `ps`, um die PID eines Prozesses herauszufinden, den man abschießen möchte. Zu diesem Zweck gibt es den `kill`-Befehl, der die gleiche Aufgabe hat wie der `taskkill`-Befehl in Windows. Der folgende Befehl beendet den Prozess mit der PID 2180:

```
mike@mike-Ubuntu:~$ kill 2180
```

Mit der Ausgabe des Befehls ps lässt sich noch viel mehr anstellen, aber das sehen wir uns im Zusammenhang mit dem nun folgenden `grep`-Befehl an.

15.4.4 grep

Der `grep`-Befehl ermöglicht, Textdateien oder Befehlsausgaben nach bestimmten Informationen zu durchsuchen oder nicht benötigte Informationen herauszufiltern. Sehen wir uns doch einmal zwei der zahllosen potenziellen Einsatzmöglichkeiten dieses leistungsfähigen Befehls an.

Mithilfe von `grep` ist es ein Kinderspiel, einen bestimmten Prozess ausfindig zu machen. Ich könnte beispielsweise ein Dokument in LibreOffice geöffnet haben und muss nun den dazugehörigen Prozess abschießen. Mir ist die PID zwar nicht bekannt, aber ich kann sie mit `ps` und `grep` herausfinden. Ich weiß, dass der Prozess das Wort »libre« enthalten muss, also gebe ich Folgendes ein:

```
mike@mike-Ubuntu:~$ ps aux | grep libre
mike      2524  0.0  0.2 145804  5652 ?        Sl   14:12   0:00 /usr/lib/
libreoffice/program/oosplash --writer
mike      2543  0.0  5.5 1140216 114080 ?      Sl   14:12   0:01 /usr/lib/
libreoffice/program/soffice.bin --writer --splash-pipe=5
```

Nun weiß ich, dass es zwei Prozesse gibt, die LibreOffice erzeugt hat: 2524 und 2543. Großartig! Der `grep`-Befehl kann nach beliebigem Text suchen und die Zeilen anzeigen, die ihn enthalten. Probieren wir den Befehl ein weiteres Mal aus, jetzt mit `ifconfig`. Nehmen wir an, Sie möchten wissen, ob irgendein Netzwerkanschluss die IP 192.168.4.15 besitzt. So verwendet man `ifconfig` zusammen mit `grep`:

```
mike@mike-Ubuntu:~$ ifconfig | grep 192.168.4.15
inet addr:192.168.4.15 Bcast:10.0.2.255 Mask:255.255.255.0
collisions:0 txqueuelen:1000
```

Wie Sie sehen zeigt `grep` eine Zeile der Ausgabe von `ifconfig` an, in der die gesuchte IP-Adresse enthalten ist.

Auch hier handelt es sich nur um einen winzigen Überblick über die Möglichkeiten, die `grep` bietet. Es ist tatsächlich eines der leistungsstärksten Werkzeuge in Linux. Wenn Sie irgendwo eine bestimmte Zeichenkette aufspüren müssen, dann ist `grep` das richtige Werkzeug.

15.4.5 apt-get/APT

In den ersten zehn Jahren nach dem Erscheinen der ersten Linux-Version konnte die Installation von Software eine ziemliche Herausforderung darstellen. Linux war schon immer ein Betriebssystem für Computerfreaks und wurde vornehmlich von Programmierern und Serveradministratoren eingesetzt. Die meisten der großen kommerziellen Softwarehersteller programmierten keine Anwendungen für Linux. Wenn man eine bestimmte Anwendung benötigte, musste man im Internet danach suchen, den Code herunterladen und versuchen, ihn auf dem eigenen System zu kompilieren, nur um dann festzustellen, dass er von weiterem Code abhängig war, der dann ebenfalls heruntergeladen werden musste. Darüber hinaus mussten die Konfigurationsdateien manuell eingerichtet werden ... Meine Güte! Es konnte wirklich mühselig sein, insbesondere im Vergleich zu der Leichtigkeit, mit der Windows- oder Mac-Programme installiert werden konnten.

Im Laufe der Jahre wurden allerdings erhebliche Fortschritte hinsichtlich der Verfügbarkeit, der Bereitstellung und der Installation von Linux-Programmen erzielt, die zur Entwicklung verschiedener sogenannter *Paketverwaltungen* führte, mit denen es möglich wurde, mit einem einzigen Befehl Software herunterzuladen, zu installieren und zu aktualisieren.

Die verschiedenen Linux-Distributionen verwenden auch unterschiedliche Paketverwaltungssysteme. Debian-basierte Linux-Distributionen (wie Ubuntu oder Mint) setzen die Paketverwaltung *APT* (*Advanced Packaging Tool*) ein. Auf Red Hat basierende Distributionen verwenden hingegen den *RPM Packet Manager* (*RPM*). Es sind natürlich noch weitere Paketverwaltungssysteme verfügbar, allerdings sind APT und RPM derzeit dominant. In den Lernzielen der CompTIA A+-Zertifizierung wird jedoch nur `apt-get` erwähnt, das Kommandozeilenprogramm zur Nutzung von APT. Damit dürfte klar sein, welche Linux-Distribution Sie nach Ansicht der CompTIA kennen sollten: Ubuntu!

`apt-get` ist wunderbar einfach verwendbar, wenn Sie wissen, wie das Programm heißt, das Sie installieren möchten. Viele Linux-Anwender sind beispielsweise keine großen Anhänger des in die Jahre gekommenen Texteditors `vi` und bevorzugen den erheblich verbesserten `vim`. Um das Programm herunterzuladen und zu installieren geben Sie zunächst folgenden Befehl ein:

```
mike@mike-Ubuntu:~$ sudo apt-get update
```

Durch diesen Befehl aktualisiert APT das Paketverzeichnis, das eine Liste aller verfügbaren Softwarepakete darstellt. Sie könnten diesen Schritt auch überspringen, aber dann installieren Sie womöglich veraltete Software oder finden ein Paket überhaupt nicht, wenn es nur neu genug ist. Nach der Aktualisierung des Paketverzeichnisses kann die eigentliche Installation stattfinden:

```
mike@mike-Ubuntu:~$ sudo apt-get install vim
```

Das war schon alles! `vim` wird nun installiert und steht danach zur Verfügung. Sie haben `vim` bereits installiert, aber nicht in der neuesten Version? Verwenden Sie `apt-get` wie folgt:

```
mike@mike-Ubuntu:~$ sudo apt-get update vim
```

Der einzige Nachteil von `apt-get` ist die Tatsache, dass Sie den Namen des Pakets kennen müssen, das Sie installieren möchten. Es gibt zwar durchaus Werkzeuge, die bei der Suche nach Software helfen können (`apt-cache`), allerdings ziehen die meisten Benutzer es vor, die grafischen Suchwerkzeuge ihrer Linux-Distribution zu verwenden, wie z.B. das Ubuntu Software-Center. So nützlich APT bei der Installation einzelner Anwendungen auch ist, die eigentliche Stärke liegt auf einem anderen Gebiet. Die Paketverwaltung handhabt *sämtliche* Software des Systems (wenn man von selbst kompilierten Programmen einmal absieht). APT ist auch das Werkzeug, mit dem Sie das gesamte System auf dem neuesten Stand halten, ebenso wie Windows Update unter Windows das System aktualisiert. Um alle auf Ihrem System vorhandenen Pakete zu aktualisieren, brauchen Sie nur die beiden folgenden Zeilen einzugeben:

```
mike@mike-Ubuntu:~$ sudo apt-get update
mike@mike-Ubuntu:~$ sudo apt-get upgrade
```

Wenn `apt-get` irgendwelche veralteten Pakete entdeckt, werden diese angezeigt und Sie werden aufgefordert, die Aktualisierung zu bestätigen. Dann werden sie heruntergeladen und installiert. Das System auf diese Weise aktuell zu halten ist wichtig, weil dadurch möglicherweise noch vorhandene Sicherheitslücken geschlossen werden.

15.4.6 vi

Früher oder später werden Sie in macOS oder Linux reine Textdateien bearbeiten müssen und `vi` ist der Standardeditor, der in macOS und den meisten Linux-Distributionen verfügbar ist. Herauszufinden, wie man mit `vi` eine Textdatei bearbeitet oder auch nur das Programm wieder beendet, kommt schon fast einem Initiationsritual gleich. Erst wenn Sie die nicht gerade intuitive oder sogar nachgerade verschrobene Bedienschnittstelle von `vi` beherrschen, dürfen Sie mit Fug und Recht von sich behaupten, ein Meister des UNIX-Terminals zu sein. Nun gut, vielleicht nicht unbedingt ein Meister, aber die Tatsache, dass `vi` praktisch auf jedem System verfügbar ist, macht es lohnenswert zu wissen, wie das Programm bedient wird. Legen Sie zunächst einmal eine Textdatei mit dem Titel `franz` an:

```
mike@mike-Ubuntu:~$ vi franz
```

Sie befinden sich nun im Editor vi und haben ein leeres Dokument vor sich (Abbildung 15.17).



Abb. 15.17: Der Editor `vi` mit leerem Dokument

Der Editor vi kennt zwei verschiedene »Modi« und befindet sich stets entweder im Eingabemodus oder im Befehlsmodus. Im Eingabemodus können Sie Text eingeben und bearbeiten. Im Befehlsmodus können Sie Befehle ausführen, wie z.B. Ausschneiden, Kopieren oder Einfügen von Text oder die Datei speichern. Nach dem Start des Programms befinden Sie sich im Befehlsmodus, drücken Sie also die Taste [I], um in den Eingabemodus zu gelangen. Geben Sie wie in Abbildung 15.18 ein paar Zeilen Text ein. Drücken Sie am Ende jeder Zeile [↵] und verwenden Sie die Taste [←], um Zeichen zu löschen, falls Sie sich vertippen. Die von anderen Texteditoren bekannten Tasten funktionieren hier nicht! Drücken Sie die [ESC]-Taste, um den Eingabemodus zu verlassen und wieder in den Befehlsmodus zu gelangen.

mike@mike-Ubuntu: ~

```
#include <stdio.h>

int main(){
    printf("Hallo Welt!\n");
    return 0;
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

Abb. 15.18: `vi` mit eingegebenem Text

Geben Sie im Befehlsmodus `ZZ` ein (zwei Großbuchstaben) und drücken Sie [↵], um die Datei zu speichern und `vi` gleichzeitig zu beenden. Geben Sie `vi` gefolgt von dem Dateinamen ein, um eine bereits vorhandene Textdatei zu bearbeiten. Wenn Sie beispielsweise die Datei `hans.txt` öffnen möchten, geben Sie ein:

```
mike@mike-Ubuntu:~$vi hans.txt
```

Der eigentliche Trick bei der Verwendung von `vi` ist, stets zu wissen, ob man sich im Befehls- oder im Eingabemodus befindet. Drücken Sie [ESC], um in den Befehlsmodus zu gelangen und [I], um in den Eingabemodus zu wechseln. Machen Sie sich darauf gefasst, dass Sie sehr viele Fehler begehen werden, wenn Sie `vi` die ersten Male benutzen.

Die in `vi` verfügbaren Kommandos sind uralt, aber durchaus leistungsfähig, wenn Sie sich die Mühe machen, sie zu erlernen. Es folgt eine Liste mit einigen Funktionen im Befehlsmodus, die sich als nützlich erweisen werden.

Taste	Funktion
h	Cursor ein Zeichen nach links bewegen
j	Cursor eine Zeile nach unten bewegen
k	Cursor eine Zeile oben unten bewegen
l	Cursor ein Zeichen nach rechts bewegen
w	Cursor ein Wort nach rechts bewegen
b	Cursor ein Wort nach links bewegen
0	Cursor an den Zeilenanfang bewegen
$	Cursor an das Zeilenende bewegen
i	Links vom Cursor einfügen
r	Aktuelles Zeichen überschreiben
dd	Aktuelle Zeile löschen
D	Zeichen vom Cursor bis zum Zeilenende löschen
x	Aktuelles Zeichen löschen
:w	Datei speichern
:q!	Programm beenden ohne zu speichern
ZZ	Datei speichern und Programm beenden

Es ist zugegebenermaßen wichtig zu wissen, wie man `vi` bedient, aber die meisten Linux-Anwender suchen sich sehr schnell eine komfortablere Alternative, von denen es Hunderte gibt. Sehen Sie sich beispielsweise die im Terminal laufenden Editoren `vim`, `joe` oder `emacs` an oder probieren Sie einen der Editoren mit grafischer Benutzeroberfläche wie gedit oder gVim aus.

15.4.7 dd

Der Befehl `dd` dient vornehmlich dazu, exakte Kopien von blockorientierten Speichergeräten in Form von Image-Dateien zu erstellen, die Bit für Bit mit dem Original übereinstimmen. Mit blockorientierten Speichergeräten sind hier Massenspeicher wie Volumes auf Festplatten, USB-Sticks oder optische Medien gemeint. In der einfachsten Form verwendet man `dd` so:

```
$ dd if=<Quelle> of=<Speicherort des Zielimages>
```

Es ist unmöglich, Ihnen alle denkbaren Anwendungsfälle zu präsentieren, für die dieser Befehl geeignet ist, daher stelle ich hier lediglich drei der gebräuchlichsten vor. Fangen wir mit etwas Einfachem an, dem Kopieren einer Festplatte.

Seien Sie vorsichtig! Nicht umsonst wird der Name `dd` scherzhaft als »Disk-Destroyer« (Festplatten-Zerstörer) interpretiert. Das Programm ist äußerst leistungsfähig, kann aber verheerenden Schaden anrichten, wenn es nicht richtig eingesetzt wird. Es gibt eine ganze Reihe von Komplikationen, die auf das Ergebnis der Verwendung des `dd`-Befehls Einfluss nehmen, die ich an dieser Stelle nicht näher erläutern kann. Die nachstehenden Kommandos funktionieren zwar prinzipiell, sie ohne Kenntnis der Einzelheiten auf Ihrem System auszuführen könnte aber auch das Löschen ganzer Laufwerke zur Folge haben. Ich habe Sie gewarnt!

Kopieren einer Festplatte

Nehmen wir an, Sie möchten den Inhalt einer Festplatte mit der Kennung `sda` auf einer anderen Festplatte mit der Kennung `sdb` speichern. In diesem Fall sollen beide Festplatten von exakt gleicher Größe sein. Der folgende Befehl kopiert die gesamte Festplatte `sda`, inklusive Partitionstabelle, Dateisystem usw. auf die Festplatte `sdb`:

```
dd if=/dev/sda of=/dev/sdb
```

Sicherungskopie eines USB-Sticks erstellen

Nehmen wir an, Sie besitzen einen USB-Stick mit der Kennung `sdc`, auf dem wichtige Daten gespeichert sind, von denen Sie eine Sicherungskopie erstellen möchten. Dann können Sie `dd` wie folgt verwenden, um eine Image-Datei (die ich hier `USBStick.bak` genannt habe) zu erstellen und auf Ihrem Desktop abzulegen:

```
dd if=/dev/sdc of=/home/mike/Desktop/USBStick.bak
```

Löschen einer Festplatte

Ich habe eine Festplatte mit der Kennung `sdb`, die ich vollständig löschen möchte. Der `dd`-Befehl kann beliebige Eingabequellen verarbeiten, daher verwende ich hier den Zufallszahlengenerator von Linux, `/dev/urandom`, als Eingabequelle, um zufällige Werte auf die gesamte Festplatte zu schreiben. Das ist zwar keine perfekte Löschung, aber man bräuchte schon sehr hochentwickelte Geräte, um die ursprünglichen Daten wieder lesbar zu machen.

```
dd if=/dev/urandom of=/dev/sdb
```

15.4.8 shutdown

Wie unter Windows können Sie das System vom Terminal aus mit dem Befehl `shutdown` herunterfahren oder neu starten. Der Befehl hat folgende Syntax:

```
shutdown <Optionen> <Zeitpunkt>
```

Als Zeitpunkt wird mit Abstand am häufigsten `now` (jetzt) angegeben. Um das System unverzüglich herunterzufahren, geben Sie diesen Befehl ein:

```
shutdown now
```

Wenn Sie das System neu starten möchten, verwenden Sie die Option `-r`:

```
shutdown -r now
```

15.4.9 passwd

Der Befehl `passwd` erlaubt es Ihnen, Ihr eigenes Kennwort oder die Kennwörter anderer Benutzer zu ändern (sofern Sie als Superuser `root` angemeldet sind). Geben Sie Folgendes ein, um Ihr eigenes Kennwort zu ändern:

```
mike@mike-Ubuntu:~$ passwd
Ändern des Passworts für mike.
(aktuelles) UNIX-Passwort:
```

```
Geben Sie ein neues UNIX-Passwort ein:
Geben Sie das neue UNIX-Passwort erneut ein:
passwd: Passwort erfolgreich geändert
```

15.5 Skriptsprachen

Bislang haben Sie Befehle auf der Kommandozeile der Reihe nach einzeln eingegeben. Meistens waren nur ein oder zwei Befehle erforderlich, aber gelegentlich werden Sie feststellen, dass Sie immer wieder die gleichen Befehlsfolgen verwenden. In diesem Fall ist es sinnvoll, ein Skript zu schreiben, das diese Befehlsfolge ausführt. Ein Skript ist ein kleines Programm, das dabei hilft, Aufgaben zu automatisieren.

Tatsächlich können Sie ein besonders einfaches Shell-Skript erstellen, indem Sie ein paar Shell-Befehle in eine Textdatei kopieren und diese speichern. Moment, Shell-Skript und Shell-Befehle? Wenn Sie Befehle auf der Kommandozeile in Windows eingeben, benutzen Sie eine Shell. Sie haben in diesem Kapitel die ganze Zeit Shell-Befehle verwendet!

Jede Shell verfügt über eine eigene Shell-Skriptsprache, deshalb hängt die Dateinamenerweiterung der Datei davon ab, welche Shell Sie verwenden. Nehmen wir an, dass es eine Anwendung namens `wichtigeapp.exe` geben muss, die wöchentlich beendet und wieder gestartet werden soll, um Wartungsarbeiten vorzunehmen zu können. Zu diesem Zweck führen Sie die folgenden Befehle aus:

```
kill /IM importantapp.exe /P gudpwd1 ❶
cd \Program files\importantapp\Data ❷
del *.tmp ❸
copy config.bak config.txt /Y ❹
wichtigeapp.exe ❺
```

❶ Beenden der Anwendung

❷ Aufsuchen eines bestimmten Verzeichnisses

❸ Temporäre Dateien löschen

❹ Konfigurationsdatei der letzten Woche mit einer Kopie des Backups überschreiben

❺ Anwendung wieder starten

Diese Befehlsfolge jede Woche einzugeben, ist mühsam, und Sie könnten sich vertippen oder sich nicht mehr richtig an sie erinnern. Legen Sie sie stattdessen in einer Textdatei ab, die Sie beispielsweise mit dem Editor anlegen können, und speichern Sie die Datei mit einer Dateinamenerweiterung ab, etwa als `wöchentlich.bat`, damit das Betriebssystem erkennt, dass es sich um ein Shell-Skript handelt.

Sie können das Skript auf der Eingabeaufforderung starten. Geschrieben haben Sie es jedoch mit einem anderen Programm, dem Editor. Das Ausführen des Skripts automatisiert die Eingabeaufforderung, denn sie wird angewiesen, eine Befehlsfolge auszuführen.

Erfahrene Techniker nutzen ständig Skripts, um alle möglichen Aufgaben zu erledigen. Mein Büro ist zwar relativ klein, aber es gibt eine Menge Computer, die dauernd irgendwelche Aufgaben erledigen. Unser Systemadministrator Michael überprüft jeden Morgen routinemäßig den Zustand all dieser Computer: Sind Fehler aufgetreten oder funktioniert alles? Das ist eine Menge Arbeit. Wenn er alle Rechner manuell überprüfen müsste, wäre er den ganzen Tag damit beschäftigt, selbst wenn die Prüfung über das Netzwerk erfolgt. Michael hat ein Skript erstellt, um die Aufgabe zu automatisieren. Er sitzt an seinem Mac, schlürft seinen Kaffee, öffnet das Terminal und führt ein paar Skripts aus, die alle Rechner überprüfen und einen ausführlichen Bericht erstellen. Klasse!

Ich möchte hier deutlich machen, dass man Skripts zwar auf der Kommandozeile ausführen kann, aber erstellt werden sie mit einem Texteditor. Windows bringt mit dem Editor bereits ein einfaches Programm dafür mit. vi und vim haben Sie in diesem Kapitel schon kennengelernt – diese Texteditoren werden in Linux häufig verwendet. Das eben erstellte Skript `wöchentlich.bat` mit der Dateiendung `.bat` verwendet eine sehr eingeschränkte Skriptsprache und wird als *Batchdatei* bezeichnet. Skripts sind jedoch nicht auf so einfache Befehle und Batchdateien beschränkt. Es gibt eine Menge verschiedener Texteditoren, mit denen beeindruckende Skripts in vielen unterschiedlichen Sprachen erstellt werden können.

15.5.1 Skripttypen und Sprachen

Die Skripterstellung ist eine Art der *Programmierung*, und eine Skriptsprache ist eine für die Erstellung von Skripts optimierte *Programmiersprache*. Wie bei jeder Art der Programmierung gibt es viele verschiedene Skriptsprachen für eine Vielzahl unterschiedlicher Aufgaben. Die Lernziele der CompTIA geben vor, dass Sie die Dateitypen für sechs verschiedene Skriptsprachen kennen müssen.

In Tabelle 15.1 sind die gebräuchlichen Skriptsprachen und ihre Dateinamenerweiterung aufgeführt.

Sprache	Dateiendung	Beschreibung
Batchdatei	.bat	Batchdateien verwenden die Skriptsprache für die Eingabeaufforderung alter Schule von Windows und DOS.
PowerShell	.ps1	PowerShell ist eine von Grund auf neu entwickelte Skriptsprache zur Automatisierung moderner Windows-Versionen. Sie ersetzt Batchdateien praktisch überall.
UNIX Shell-Skript	.sh	Gemäß Konvention gibt die erste Zeile eines Shell-Skripts für UNIX an, welche Shell das Skript ausführen soll (und somit auch, in welcher Skriptsprache es geschrieben wurde). Die Dateinamen enden häufig (aber nicht immer) auf `.sh`.
Python	.py	Python ist eine flexible Programmiersprache mit einfacher Syntax und sowohl für einfache Skripts als auch für große Anwendungen gut geeignet.
JavaScript	.js	JavaScript ist eine Skriptsprache für Webbrowser, die in den 1990er-Jahren zur Erweiterung von Webseiten entwickelt wurde, wird heutzutage aber auch für Kommandozeilenprogramme, Programmerweiterung und vieles andere mehr verwendet.
Visual Basic Script	.vbs	Visual Basic Script ist eine ältere Skriptsprache für Windows und andere Programme von Microsoft. Sie wird allmählich durch andere Sprachen wie PowerShell abgelöst.

Tabelle 15.1: Gebräuchliche Skriptsprachen und ihre Dateiendungen

Hinweis

Die ersten drei Sprachen in Tabelle 15.1 sind Shell-Skriptsprachen, die anderen hingegen sind allgemeinere Skriptsprachen. Bei einer Shell-Skriptsprache ist jeder Befehl, den man in der Eingabeaufforderung eingeben kann, ein gültiger Bestandteil der Sprache. Das trifft für die allgemeineren Skriptsprachen nicht zu, die aber viele andere nützliche Features bieten.

15.5.2 Aufbau eines Skripts

Eine Programmiersprache kann einen Computer anweisen, mit bestimmten Daten irgendetwas anzustellen. Sie haben bereits Matheaufgaben gelöst, das ist schon die halbe Miete. Bei einer einfachen

Aufgabe wie `3+4` gibt es zwei Zahlen und ein Symbol, das angibt, welche Operation ausgeführt werden soll. In diesem Fall ist es eine Addition.

Wichtig

Gemäß den Lernzielen der CompTIA sollten Sie in der Lage sein, einige der grundlegenden Merkmale eines Skripts zu erkennen. Keine Sorge! Sie brauchen nicht zu wissen, wie man ein Skript schreibt oder darin enthaltene Fehler behebt. Vergewissern Sie sich aber, dass Ihnen die hier beschriebenen Bestandteile geläufig sind.

Um die Aufgabe lösen zu können, müssen Sie die Rechenregeln kennen, die Sie schon in der Grundschule gelernt haben. Die beiden Zahlen sind *Werte*, und die Regeln besagen, dass zwei Werte addiert werden, wenn ein Pluszeichen dazwischen steht.

Und wenn die Aufgabe ein wenig anders aussieht? Was würden Sie tun, wenn die Aufgabe `3+Kuh` lautet? Ergibt das einen Sinn? `Kuh` ist keine Zahl, sondern eine Bezeichnung für ein großes, grasfressendes Rind. Sie und ich wissen das, aber für den Computer sind `3` und `Kuh` nur ein paar Zeichen. Wie erkennt er, dass eine Addition nicht möglich ist?

15.5.3 Datentypen

Damit Computer Zahlen und Wörter unterschiedlich behandeln, ist ein neues Konzept erforderlich, nämlich *Datentypen*. Ein Datentyp beschreibt eine festgelegte Kategorie, wie beispielsweise *Zahl* oder *Wort*. In vielen Programmiersprachen gibt es Regeln, die wichtige Details festlegen, etwa dass man die Zahl 3 und das Wort Kuh nicht addieren kann, weil es sich um unterschiedliche Datentypen handelt. Die Zahl 3 ist ein *Integer* (also eine Ganzzahl), und Kuh ist das, was Programmierer als *String* bezeichnen. Jetzt wird es ein klein wenig komplizierter, aber gleich wird alles verständlich.

Einen String können Sie sich wie eine Zeichenkette vorstellen, wie z.B. K-u-h. In den meisten Programmiersprachen ist es erforderlich, Strings in einfache oder doppelte Anführungszeichen einzuschließen: `'Kuh'` oder `"Kuh"`. Nur einige wenige Zeichen sind gültige Integers, ein String hingegen kann alle möglichen Zeichen enthalten. In allen Programmiersprachen gibt es Aktionen, die mit Strings ausgeführt werden können, wie etwa zwei Strings miteinander zu verknüpfen, einen String in mehrere Teile zu zerlegen, zu berechnen, wie viele Zeichen ein String enthält, und so weiter. Die Regeln besagen, dass 3 und Kuh nicht addiert werden können (vielleicht würde es die Kuh verärgern), Sie können aber sehr wohl `"schwarzbunte " + "Kuh"` bilden und erhalten auf diese Weise eine `"schwarzbunte Kuh"` (die hoffentlich glücklicher ist).

Wichtig

In den Lernzielen der CompTIA werden nur zwei grundlegende Datentypen erwähnt, nämlich Integers und Strings. In manchen Programmiersprachen gibt es weitere Datentypen für bestimmte Zwecke (wie etwa Datentypen für Kalenderdaten oder Bruchzahlen), diese brauchen Sie für die Prüfung aber nicht zu kennen.

Jetzt kommt das nächste coole Konzept. Zahlen bestehen ja, ebenso wie Wörter, aus Zeichen. Deshalb können Strings Zahlen enthalten – und Programmiersprachen müssen mit den Zahlenzeichen unterschiedlich verfahren, je nachdem, ob sie in Anführungszeichen stehen oder nicht. Eine Programmiersprache muss deshalb festlegen, wie sie mit einer Telefonnummer verfährt, die ohne oder mit Anführungszeichen angegeben ist. Hier ist ein Beispiel:

```
281-922-4166
"281-922-4166"
```

Bei der ersten Schreibweise hätte der Computer keine andere Wahl, als das Ergebnis von 281 minus 922 minus 4166 zu berechnen, was -4807 ergibt (Datentyp Integer). Bei der zweiten Schreibweise würde der String, der die Telefonnummer meines Büros enthält, intakt bleiben.

15.5.4 Variablen

Sobald der Computer die Verwendung dieses Wertes abgeschlossen hat (sei es nun -4807 oder "281-922-4166"), wird er dies vergessen. Wenn Sie ihn mehrmals verwenden möchten, müssen Sie den Computer anweisen, ihn zu speichern. In den meisten Programmiersprachen erfolgt das dadurch, dass man den Wert benennt. Diese benannten Werte werden als *Variablen* bezeichnet. Die Telefonnummer meines Büros wird in der Variablen `telefon_büro` gespeichert:

```
telefon_büro = "281-922-4166"
```

15.5.5 Bedingte Anweisungen und einfache Schleifen

Wenn man die allereinfachsten Shell-Skripts, die nur aus einer Liste von Befehlen bestehen, hinter sich gelassen hat, muss man oft steuern können, wann und wie bestimmte Befehle ausgeführt werden. Umfassendere Skript- und Programmiersprachen stellen zu diesem Zweck *Kontrollstrukturen* bereit.

Hinweis

Dieser Abschnitt enthält einige Beispielskripte, die *Python* verwenden. Wenn Sie versuchen, diese in eine Skriptdatei für eine andere Sprache zu kopieren, werden sie wahrscheinlich nicht funktionieren.

Die einfachsten Kontrollstrukturen sind bedingte Anweisungen. Sie ermöglichen es, Code anzugeben, der nur dann ausgeführt werden soll, wenn eine bestimmte Bedingung erfüllt (oder nicht erfüllt) ist. In den meisten Sprachen gibt es Schlüsselwörter, wie beispielsweise das »if« in einer `if`-Anweisung, mit dem die Bedingung festgelegt und der Code angegeben wird, der ausgeführt werden soll, wenn die Bedingung erfüllt ist. Hier ist ein einfaches Beispiel:

```
tier = "Kuh"
if tier == "Katze":
    print("Miau")
```

Die Zeilen haben folgende Bedeutung:

1. Die Variable `tier` enthält den String `"Kuh"`.
2. Die `if`-Anweisung überprüft, ob die Variable `tier` den Wert `"Katze"` enthält.
3. Wenn das der Fall ist, gibt der Computer auf der Kommandozeile das Wort `"Miau"` aus. Wenn nicht, passiert nichts weiter.

Im vorliegenden Fall würde das Skript nichts ausgeben, weil die Bedingung nicht erfüllt ist.

Bedingte Anweisungen sind für die meisten Skripts und Programme unverzichtbare Bausteine. Dass man eine bestimmte Aufgabe viele Male ausführen möchte, ist einer der wichtigsten Gründe, überhaupt ein Skript zu schreiben. Das kann man bei der Programmierung durch eine Schleife erreichen. Einfache Schleifen sind auch bedingte Anweisungen, weisen den Computer jedoch an, den Code immer wieder auszuführen, bis eine Bedingung erfüllt (oder nicht erfüllt) ist. Es hängt von der verwendeten Sprache ab, aber die meisten verwenden für Schleifen die Schlüsselwörter `for` und `while`. Hier ist wieder ein Beispiel:

```
kühe = 0
while kühe < 4:
    print ("Muh")
    kühe = kühe + 1
```

Die Schleife wird so lange wiederholt, bis die Anzahl der Kühe vier ist, es wird also vier Mal `"Muh"` ausgegeben – einmal pro Kuh. Da die Variable einen Integer-Wert enthält, können Sie mit ihr rechnen. Bei jedem Schleifendurchlauf wird `"Muh"` ausgegeben und die Anzahl der Kühe um eins erhöht.

Wichtig

Verschiedene Programmiersprachen verfügen über unterschiedliche Kontrollstrukturen. Die meisten besitzen davon zumindest eine Handvoll. In diesem Abschnitt haben wir zwei betrachtet, `if`-Anweisungen und Schleifen. Den Lernzielen der CompTIA zufolge müssen Sie nur einfache Schleifen kennen.

15.5.6 Kommentare

Skript- und Programmiersprachen stellen für gewöhnlich eine Möglichkeit zur Verfügung, *Kommentare* anzugeben. Sie sollen dem Betrachter des Skripts später dabei helfen, zu verstehen, was eigentlich vor sich geht. (Das gilt auch für den Autor, wenn inzwischen ein paar Monate vergangen sind!) Der Computer ignoriert Kommentare – sie sind ausschließlich für Menschen gedacht. Kommentare zu erstellen, ist wirklich eine gute Idee, auch wenn Sie nicht damit rechnen, dass irgendjemand anderes Ihr Skript jemals lesen wird. Kommentare bieten die Möglichkeit, zu beschreiben, welche Aufgaben das Skript eigentlich erledigen soll. Sie können in den Kommentaren auch erläutern, wie, wann und wo das Skript anwendbar ist.

Jede Sprache verwendet eine eigene Syntax, allerdings nutzen die meisten Sprachen zwei Formate. Bei drei der Sprachen, die Sie gemäß den CompTIA-Lernzielen kennen sollten (PowerShell, Python und UNIX-Shell), beginnen Kommentare mit dem Symbol #. Das Kommentarsymbol kann am Anfang einer Zeile stehen oder Anweisungen in der gleichen Zeile folgen. Das sieht so aus:

```
# Dieses Skript bringt alle Kühe zum Muhen.
# Vorsicht – es ist mächtig.
kühe = 0 # Am Anfang gibt es keine Kühe
while kühe < 4: # Nur vier Kühe dürfen muhen :(
    print() # Muh, Kuh, Muh!
    kühe = kühe +1 # Eine Kuh hinzufügen
```

Die Kommentare in diesem Beispiel beschreiben die Aufgabe des Skripts, warnen den Benutzer, merken an, dass es zunächst keine Kühe gibt, und so weiter.

Die Kommentare in den anderen drei Sprachen unterscheiden sich jeweils ein wenig und lassen sich somit auseinanderhalten.

JavaScript:

```
// Ein einzeiliger Kommentar in JavaScript
/* Ein mehrzeiliger Kommentar
in JavaScript */
```

Batchdatei:

```
REM Das ist eine ältere Methode für Kommentare.
:: Neuere Skripte verwenden dieses Format.
```

Visual Basic Script:

```
' Kommentare beginnen mit einem einfachen
' Anführungszeichen.
```

Bei der Skripterstellung und Programmierung sind Kommentare für die Menschen, die sich damit befassen, unverzichtbar. Nichts ist schlimmer, als sich daran erinnern zu müssen, wie viele Kühe muhen werden, wenn die Skripterstellung ein Jahr her ist!

15.5.7 Umgebungsvariablen

Alle Systeme, auf die Sie zugreifen, speichern wichtige Werte in Variablen, die die sogenannte *Umgebung* eines Programms bilden. Einige dieser Variablen sind systemweit gültig, diese Werte können aber vom Benutzer, einem Skript/Programm oder auch durch die Shell, in der ein Skript abläuft, geändert werden.

Diese Werte, die *Umgebungsvariablen*, liefern den laufenden Programmen alle möglichen Informationen, beispielsweise das aktuelle Arbeitsverzeichnis des Benutzers oder wo temporäre Dateien gespeichert werden. Abbildung 15.19 zeigt die Standardumgebungsvariablen für Programme, die unter einem Benutzerkonto ausgeführt werden.

Wir verwenden Umgebungsvariablen auch dazu, Skripts zu konfigurieren, weil sie es erleichtern, das Verhalten des Skripts für viele verschiedene Benutzer anzupassen, ohne es selbst ändern zu müssen. Hier ist ein Beispiel für die Verwendung von Umgebungsvariablen in einer Batchdatei (`REM` leitet einen Kommentar ein):

```
@echo off
REM Gibt den Namen des aktuell angemeldeten Benutzers aus
echo Sie sind angemeldet als %username%
REM Gibt das Heimverzeichnis des aktuellen Benutzers aus
echo Ihr Heimverzeichnis ist %homepath%
```

Die von Prozentzeichen umschlossenen Bezeichnungen (wie `%username%`) sind Umgebungsvariablen, die sich in Abhängigkeit vom Benutzer, der die Batchdatei ausführt, ändern. Wenn ich das Skript ausführe, hat die Variable den Wert »Mike«, wenn mein Redakteur es ausführt, erhält sie den Wert »Scott«.

In macOS und Linux gibt es ähnliche Umgebungsvariablen wie in Windows, sie sehen jedoch ein wenig anders aus. Hier ist das gleiche Skript für ein macOS-System:

```
#!/bin/bash
# Gibt den Namen des aktuell angemeldeten Benutzers aus
echo Sie sind angemeldet als $USER
# Gibt das Heimverzeichnis des aktuellen Benutzers aus
echo Ihr Heimverzeichnis ist $HOME
```

Erfahrene Techniker verwenden Skripts, um viele alltägliche Aufgaben schnell und effizient auszuführen. Mit Skripts können Sie den Rechner auf vielfältige Weise steuern. Für die CompTIA-Zertifizierungsprüfung sollten Sie die in diesem Kapitel vorgestellten Konzepte kennen, aber was man mit Skripts alles anstellen kann, wird Sie umwerfen. Probieren Sie es aus!

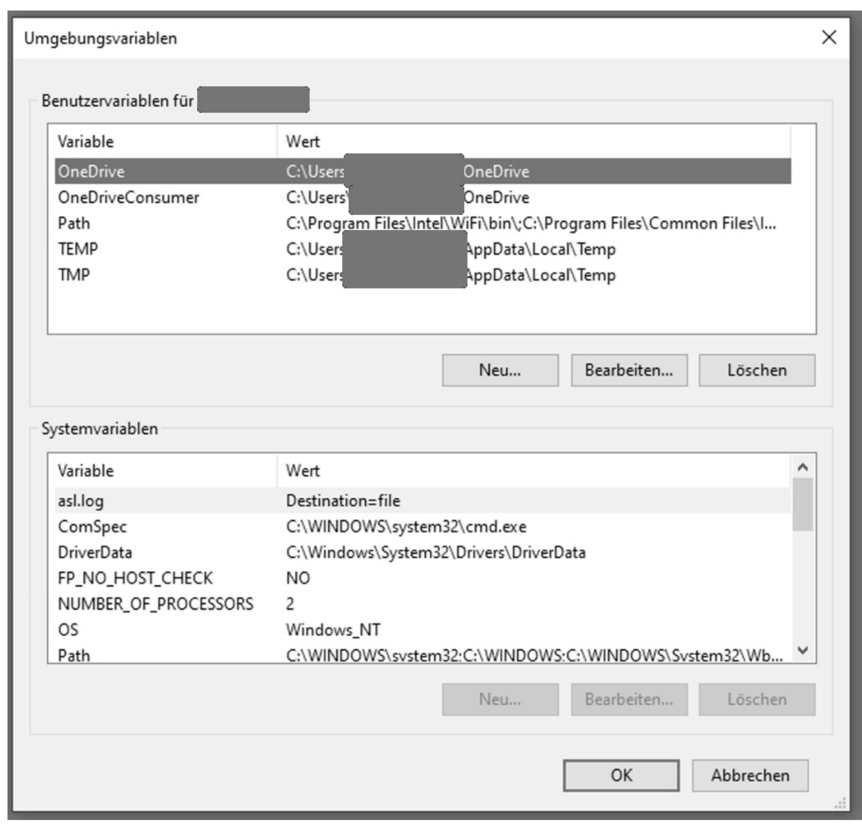


Abb. 15.19: Umgebungsvariablen in Windows 10

15.6 Wiederholung

15.6.1 Fragen

1. Welches der folgenden Zeichen ist in einem Dateinamen in Linux nicht erlaubt?
   A. * (Stern)
   B. . (Punkt)
   C. / (Schrägstrich)
   D. _ (Unterstrich)
2. Welcher Befehl gibt den Inhalt eines Verzeichnisses seitenweise aus? (Wählen Sie zwei Antworten aus.)
   A. `dir p`
   B. `ls | more`
   C. `ls -p`
   D. `dir /p`
3. Welcher Befehl löscht in Linux alle Dateien in einem Ordner?
   A. `del *.*`
   B. `del all`

C. `rm *`
D. `rm all`

4. Welcher Befehl gibt in Linux das aktuelle Arbeitsverzeichnis aus?
   A. `dir`
   B. `path`
   C. `pwd`
   D. `prompt`
5. Welcher Windows-Befehl entspricht dem Linux-Befehl `ls`?
   A. `dir`
   B. `command`
   C. `copy`
   D. `dd`
6. Was müssen Sie vor dem Namen eines Linux-Befehls eingeben, um auf die zugehörigen Hilfeseiten zuzugreifen?
   A. `help`
   B. `?`
   C. `man`
   D. `/?`
7. Welcher der folgenden Linux-Befehle zeigt ausführliche Informationen über den Inhalt eines Ordners an
   A. `ls -l`
   B. `ls -e`
   C. `ls -h`
   D. `ls -k`
8. Welcher in Windows und Linux gleichlautende Befehl zeigt Ihnen den Namen des Computers an?
   A. `hosts | grep`
   B. `whoami`
   C. `hostname`
   D. `net name`
9. Wie lässt sich die Funktion des Windows-Befehls `gpresult` am besten beschreiben?
   A. Liste der kürzlich aktualisierten Gruppenrichtlinien
   B. Liste der auf einen Benutzer angewendeten Gruppenrichtlinien
   C. Liste aller Änderungen der Gruppenrichtlinien eines Benutzers seit der letzten Aktualisierung
   D. Liste aller einander widersprechenden Gruppenrichtlinien
10. Wie kann man einen Befehl in der Eingabeaufforderung von Windows mit Administratorrechten ausführen?
   A. Auf der Befehlszeile Benutzernamen und Kennwort eines Benutzerkontos mit Administratorrechten eingeben
   B. Mit der rechten Maustaste auf eine Verknüpfung mit der Eingabeaufforderung klicken und ALS HAUPTBENUTZER AUSFÜHREN auswählen
   C. Mit der rechten Maustaste auf eine Verknüpfung mit der Eingabeaufforderung klicken und ALS ADMINISTRATOR AUSFÜHREN auswählen
   D. Der Befehl kann nur von einem Benutzerkonto mit Administratorrechten ausgeführt werden

15.6.2 Antworten

1. **C.** Alle diese Zeichen sind in Linux-Dateinamen erlaubt, nur der Schrägstrich nicht, der ausschließlich zur Trennung von Verzeichnisnamen in Pfadangaben verwendet wird.
2. **B, D.** Die Befehle `ls | more` bzw. `dir /p` geben in Linux oder Windows den Inhalt eines Verzeichnisses seitenweise aus.
3. **C.** Geben Sie `rm *` ein und drücken Sie ↵, um alle Dateien in einem Linux-Verzeichnis zu löschen.
4. **C.** Der Befehl `pwd` (*print working directory*) zeigt das Arbeitsverzeichnis in Linux an.
5. **A.** In Windows erledigt der Befehl `dir` die gleiche Aufgabe wie der Befehl `ls` in Linux.
6. **C.** In Linux greift man durch Eingabe von `man [Befehlsname]` auf die Hilfeseiten zu.
7. **A.** Geben Sie `ls -l` ein und drücken Sie ↵, um in Linux ausführliche Informationen über den Inhalt eines Ordners anzuzeigen.
8. **C.** Geben Sie `hostname` ein und drücken Sie ↵, um den Namen des Computers anzuzeigen.
9. **B.** In Windows zeigt der Befehl `gpresult` eine Liste der auf einen Benutzer angewendeten Gruppenrichtlinien an.
10. **C.** Um einen Befehl in der Eingabeaufforderung von Windows mit Administratorrechten auszuführen, klicken Sie mit der rechten Maustaste auf eine Verknüpfung mit der Eingabeaufforderung und wählen ALS ADMINISTRATOR AUSFÜHREN aus.

Fehlerbehebung 16

Themen in diesem Kapitel:

- Fehlerbehebung beim Systemstart
- Fehlerbehebung bei Problemen mit der grafischen Benutzerschnittstelle
- Fehlersuche bei Problemen mit Programmen

In diesem Kapitel werden die Probleme, die bei Betriebssystemen auftreten können, von Grund auf betrachtet. Es beginnt mit katastrophalen Fehlern, bei denen der PC nicht bootet, und beschreibt dann, wie derartige Probleme gelöst werden können. Im nächsten Abschnitt geht es um Ursachen und Lösungen für den Fall, dass die grafische Benutzeroberfläche nicht startet. Sobald die GUI dann geladen wird, stehen Ihnen alle Diagnose- und Fehlersuchwerkzeuge zur Verfügung, über die Sie bereits so viel gelernt haben. Abschließend werden die verschiedenen Probleme betrachtet, die es mit Anwendungen geben kann.

Die CompTIA A+-Zertifizierungsprüfung 1002 konzentriert sich vornehmlich auf die Fehlerbehebung in Windows, daher orientiert sich die grundlegende Struktur dieses Kapitels an diesem Beispiel. Ich betrachte die verschiedenen möglichen Probleme zunächst aus der Perspektive eines PC-Technikers, der aktuelle Windows-Betriebssysteme betreut, und erörtere dann, sofern es vergleichbare Probleme gibt, die Symptome, Werkzeuge und Vorgehensweisen in macOS und Linux.

Die unter Windows auftretenden Probleme gibt es auch in macOS und Linux, wie etwa defekte Hardware oder Fehler im Betriebssystem, in Treibern und in Anwendungen. Die Vorgehensweisen bei der Fehlerbehebung der drei Betriebssystemfamilien unterscheiden sich jedoch deutlich.

Es gibt eine Unzahl von Unternehmen, die für Windows Hardware herstellen oder Software schreiben. Das dadurch entstehende *heterogene Ökosystem* (soll heißen: die große Vielgestaltigkeit) von Windows-Systemen erhöht die Anzahl der denkbaren Fehlerquellen, die Probleme verursachen können, erheblich.

Da Apple die zum Betrieb von macOS eingesetzte Hardware und die dazugehörigen Treiber schon immer streng kontrolliert hat, lässt sich fehlerhafte Hardware leichter diagnostizieren. Gleiches gilt für Probleme mit Anwendungen in macOS, weil es sich hier im Vergleich mit Windows um ein ziemlich *homogenes Ökosystem* handelt; es gibt also keine so große Vielgestaltigkeit. Wenn man von Erweiterungen des Arbeitsspeichers einmal absieht, wird die Hardware der meisten Rechner, auf denen macOS läuft, kaum aufgerüstet. Dadurch werden die Probleme umgegangen, von denen Windows-Rechner geplagt werden. Darüber hinaus liefert Apple zusammen mit dem eigentlichen Betriebssystem eine Menge ausgezeichneter Produktivitätsanwendungen aus, sodass für die meisten Anwender kaum ein Anreiz besteht, zusätzliche Software zu installieren. Dadurch werden ebenfalls Probleme vermieden.

Auf im Produktivbetrieb eingesetzten Linux-Rechnern, im Allgemeinen sind das Server, ist die übermäßige Komplexität oft gar nicht vorhanden, die bei Rechnern, auf denen Windows oder macOS läuft, häufig anzutreffen ist. Linux-Server laufen daher oft äußerst stabil. Wenn Sie das mit den von Enthusiasten (oder Dilettanten) zusammengeschusterten Systemen vergleichen, die ein Großteil von uns benutzt, treten hier alle möglichen Probleme auf. Das liegt wohl daran, dass in den meisten dieser Systeme irgendwelche übrig gebliebenen Komponenten älterer Windows-Rechner verbaut sind. Qualität hat nun mal ihren Preis, würde ich sagen.

Das Kapitel beschreibt die gängigen Probleme mit Betriebssystemen sowie die Werkzeuge und üblichen Lösungen, die in den Lernzielen 1.5, 1.6 und 3.1 der Zertifizierungsprüfung 1002 aufgeführt sind. Befassen wir uns also nun mit der Fehlerbehebung.

1002

16.1 Das System startet nicht

Wenn ein Computer nicht startet, müssen Sie zunächst feststellen, ob es sich um ein Problem der Hardware oder der Software handelt. Wie Sie aus Kapitel 9 wissen, muss die Festplatte korrekt angeschlossen sein und mit Strom versorgt werden. Und auch das CMOS muss richtig konfiguriert sein. Ist dem nicht so, erhalten Sie eine Anzeige wie in Abbildung 16.1. Wir sehen uns das gleich als kleine Auffrischung etwas genauer an.

```
Operating System not found
_
```

Abb. 16.1: Wenn Sie diese Fehlermeldung sehen, liegt ein Hardwareproblem vor. Windows hat überhaupt noch nicht versucht zu starten.

Wenn die Festplatte jedoch läuft und der POST erfolgreich abgeschlossen wurde, versucht der Computer, ein Betriebssystem zu laden. Tritt an *dieser* Stelle ein Problem auf, erhalten Sie völlig anders geartete Fehlermeldungen, wie etwa `BOOTMGR is missing` (BOOTMGR nicht gefunden, siehe Abbildung 16.2). Dementsprechend müssen Sie auch ganz andere Werkzeuge verwenden als bei der Fehlerbehebung im Zusammenhang mit Hardwareproblemen oder der CMOS-Konfiguration.

```
BOOTMGR is missing
Press Ctrl+Alt+Del to restart
_
```

Abb. 16.2: Beängstigende Fehlermeldung

16.1.1 Hardware und Konfiguration

Bei den meisten missglückten Startvorgängen müssen Sie feststellen, ob der Fehler in der Hardware oder der CMOS-Konfiguration begründet ist oder ob er unter Windows auftritt. Das lässt sich für gewöhnlich leicht überprüfen. Wenn ein Anwender Sie anruft und sagt: »Mein PC startet nicht« oder »Mein Computer gibt keine Lebenszeichen mehr von sich«, dann sind die besten Hilfsmittel eine genaue Kenntnis des Startvorgangs und das Stellen vieler Fragen, wie die folgenden:

- Was wird auf dem Bildschirm nach dem Einschalten angezeigt?
- Hören Sie irgendetwas nach dem Einschalten?
- Ist der PC mit der Steckdose verbunden?
- Riecht es merkwürdig?

Bei manchen Hardwaredefekten bleibt der Bildschirm leer, folgen Sie daher der bewährten Methode zur Fehlerbehebung. Stellen Sie sicher, dass alles korrekt angeschlossen und eingeschaltet ist. Wenn es sich um ein neues Gerät handelt (jünger als 30 Tage), könnte es sich um einen Burn-in-Fehler handeln, ein selten auftretendes Problem, das alle elektronischen Geräte betreffen kann. Wenn es merkwürdig riecht, ist möglicherweise eine der Komponenten durchgebrannt. Versuchen Sie testweise, RAM-Bausteine, Netzteil, CPU, Festplatte oder Mainboard durch bekanntermaßen funktionierende Bauteile zu ersetzen.

Falls der Anwender erklärt, dass auf dem Bildschirm `No boot device detected` (Kein Startlaufwerk erkannt) angezeigt wird, das System aber vorher einwandfrei funktioniert hat, *kann* dies auf einfache Probleme hinweisen, beispielsweise dass der Computer versucht, von einer falschen Festplatte zu starten, die vielleicht nicht die Primärpartition ist. Das geschieht öfter, als man denkt! Jemand schließt

einen USB-Speicherstick an und die Startreihenfolge im CMOS ist so festgelegt, dass der Computer zunächst versucht, von einem Wechseldatenträger zu starten statt von der Festplatte. Als mir das zum ersten Mal passierte, hätte ich fast den kompletten Rechner zerlegt, bevor mir ein Licht aufging. Nach dem Entfernen des USB-Speichersticks startete Windows wieder ganz normal.

Startprobleme unter Windows

Unter Windows gibt es zwei entscheidende Dateien, die der Gefahr ausgesetzt sind, beschädigt zu werden, nämlich `bootmgr` und `bcd`, die sich beide mit demselben Werkzeug namens `bcdedit` reparieren lassen. Das Programm ist in der Windows-Wiederherstellungsumgebung verfügbar.

WinPE

Mit Windows Vista hat Microsoft die vorher von allen Windows-Versionen verwendete, textbasierte 16-Bit-Installationsumgebung auf 32-Bit bzw. 64-Bit aktualisiert. Die Installation erfolgt nun mit einer grafischen Benutzeroberfläche und unterstützt Mauszeiger und anklickbare Elemente, anstatt Kommandozeilenwerkzeuge einzusetzen. Microsoft bezeichnet diese Installationsumgebung als *Windows-Vorinstallationsumgebung* (*WinPE – Windows Preinstallation Environment*).

Dank WinPE können Sie direkt von den Windows-Medien (DVD oder USB-Speicherstick) starten. Es wird dann ein funktional eingeschränktes, grafisches Betriebssystem geladen, das (neben der Möglichkeit, das System zu installieren) sowohl Werkzeuge zur Fehlerbehebung als auch Diagnosetools mitbringt.

Hinweis

Ich erläutere an dieser Stelle nur die Fehlerbehebung bei Startproblemen, WinPE kann aber noch mehr. Es unterstützt auch unbeaufsichtigte Installationen, Installationen über das Netzwerk und sogar den Start festplattenloser Rechner im Netzwerk.

Wenn Sie auf die Fehlerbehebungs- und Reparaturfunktionen von WinPE zugreifen, verwenden Sie eine spezielle Sammlung von Werkzeugen, die als *Windows-Wiederherstellungsumgebung* (*WinRE – Windows Recovery Environment*) bezeichnet wird. Die Begriffe sind hier aufgrund der Ähnlichkeit leicht zu verwechseln. Merken Sie sich am besten: WinRE ist das Reparaturwerkzeug in WinPE. WinPE ermöglicht WinRE. Alles klar?

Wichtig

Microsoft bezeichnet WinRE auch als *Systemwiederherstellungsoptionen.*

Windows RE

WinRE umfasst eine beeindruckende, leistungsfähige Sammlung automatisierter und manuell arbeitender Werkzeuge, die in ihrer Gesamtheit auch die schwierigsten Startprobleme von Windows diagnostizieren und reparieren können. WinRE erledigt zwar die Arbeit für Sie, dennoch müssen Sie wissen, wie Sie darauf zugreifen und es verwenden können. Bei Startproblemen von Windows ist WinRE eines der bedeutsamsten Werkzeuge.

Start von Windows RE

Unter Windows 7 gibt es drei Methoden, um auf WinRE zuzugreifen. Erstens können Sie von der Installations-DVD starten und REPARIEREN auswählen. Zweitens können Sie im Menü ERWEITERTE STARTOPTIONEN (F8) COMPUTER REPARIEREN auswählen (Abbildung 16.3). Und drittens können Sie einen *Systemreparaturdatenträger* erstellen, bevor Sie Startprobleme bekommen. Öffnen Sie dazu in der Systemsteuerung das Applet SYSTEM UND SICHERHEIT|SICHERN UND WIEDERHERSTELLEN und wählen Sie dann SYSTEMREPARATURDATENTRÄGER ERSTELLEN aus.

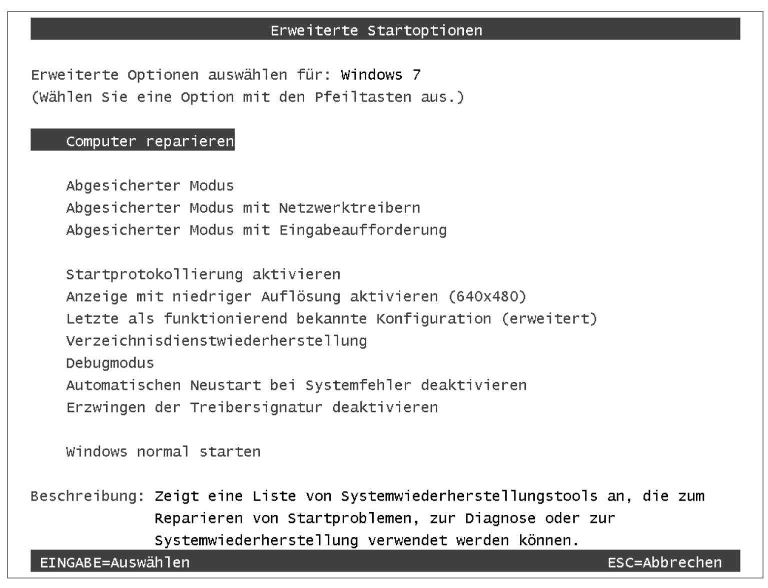


Abb. 16.3: Auswahl von COMPUTER REPARIEREN im Menü ERWEITERTE STARTOPTIONEN

In Windows 8/8.1/10 gibt es standardmäßig keine ERWEITERTEN STARTOPTIONEN (F8) und auch kein Applet SICHERN UND WIEDERHERSTELLEN. Stattdessen können Sie mit dem Applet WIEDERHERSTELLUNG in der Systemsteuerung ein Wiederherstellungslaufwerk auf einem mindestens 16 GB großen USB-Speicherstick erstellen (Abbildung 16.4). Die Erweiterten Startoptionen sind wohlgemerkt noch vorhanden, aber Microsoft hat den einfachen Zugriff über die Taste F8 entfernt. Starten Sie vom Wiederherstellungslaufwerk, um auf WinRE zuzugreifen. (Es gibt verschiedene Möglichkeiten, WinRE aufzurufen, sobald Sie auf Ihren Windows-Desktop zugreifen können, aber in diesem Abschnitt wird davon ausgegangen, dass dies nicht möglich ist.)

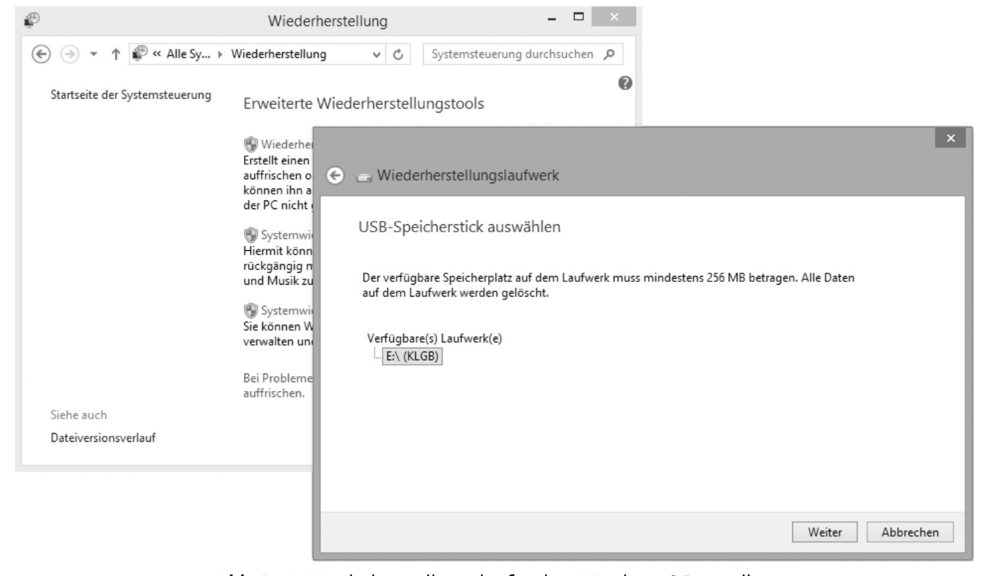


Abb. 16.4: Wiederherstellungslaufwerk in Windows 8.1 erstellen

In Windows 10 können Sie Windows-Installationsmedien erstellen, indem Sie diese direkt von Microsoft herunterladen und einen startfähigen USB-Speicherstick erstellen. Hier ist die derzeitige URL: `https://www.microsoft.com/de-de/software-download/windows10`.

Alternativ können Sie nach *Windows Media Creation Tool* suchen, um auf die entsprechende Seite zu gelangen. Schließen Sie einen USB-Speicherstick an und klicken Sie auf TOOL JETZT HERUNTERLADEN, um einen startfähigen USB-Stick zu erstellen, mit dem Sie auf Win PE zugreifen können (Abbildung 16.5).

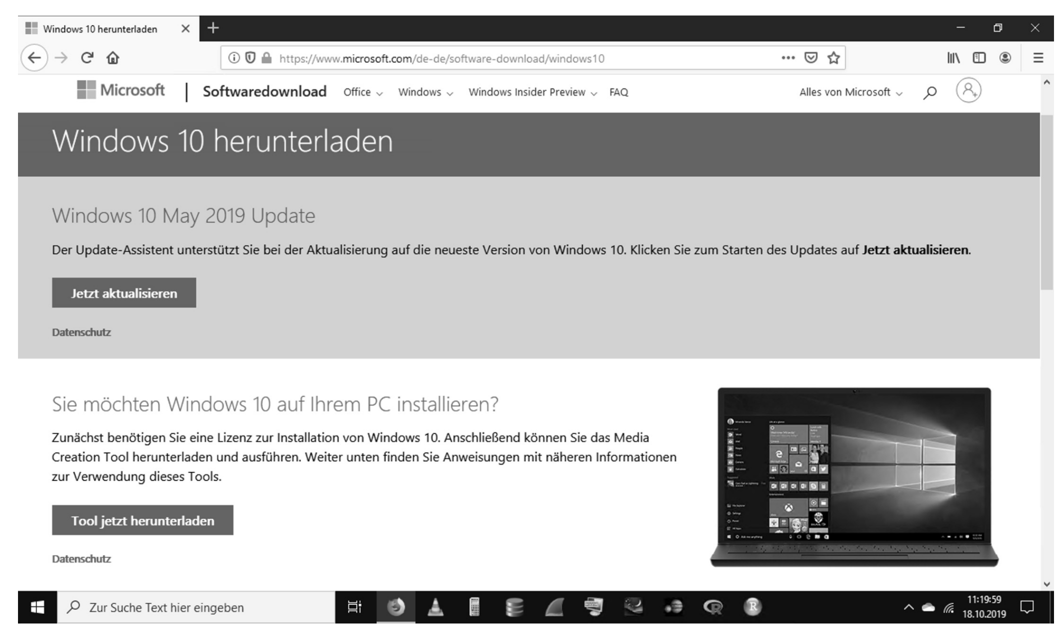


Abb. 16.5: Windows 10 herunterladen

Auch wenn alle diese Methoden normalerweise problemlos funktionieren, empfehle ich aus drei Gründen, auf WinRE über die Installationsmedien oder ein Wiederherstellungslaufwerk zuzugreifen:

- Die Festplatte könnte bereits so stark beschädigt sein, dass Sie das Menü ERWEITERTE STARTOPTIONEN gar nicht mehr aufrufen können.
- Für den Aufruf von WinRE über die Option COMPUTER REPARIEREN im Menü ERWEITERTE STARTOPTIONEN ist ein Administratorkennwort erforderlich.
- Durch die Verwendung einer startfähigen Disc oder eines USB-Speichersticks umgehen Sie möglicherweise auf dem System vorhandene Schadsoftware.

Window RE verwenden

Das Aussehen von Windows RE in Windows 7 unterscheidet sich deutlich von demjenigen in Windows 8/8.1/10, allerdings finden sich ähnliche Optionen. In Windows 7 gibt es eine einfache Bedienoberfläche mit fünf Optionen (Abbildung 16.6):

- Systemstartreparatur
- Systemwiederherstellung
- Systemabbild-Wiederherstellung
- Windows-Speicherdiagnose
- Eingabeaufforderung

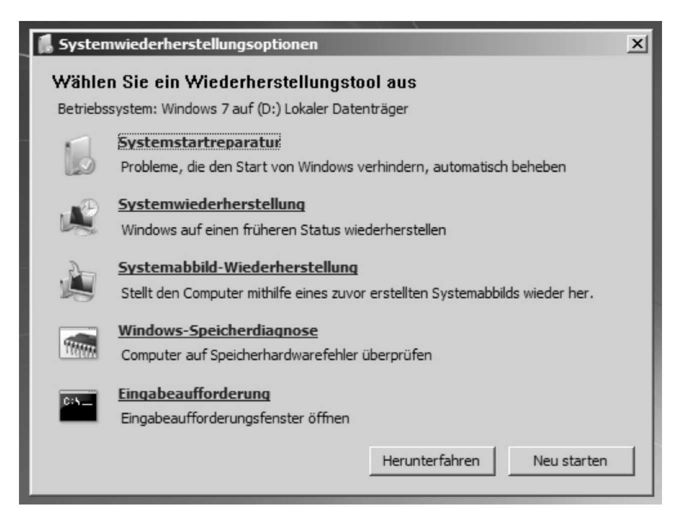


Abb. 16.6: Hauptbildschirm der Wiederherstellungsumgebung in Windows 7

In Windows 8/8.1/10 bietet WinRE eingangs weniger Optionen. Das Hauptmenü (Abbildung 16.7) bietet folgende Optionen:

- FORTSETZEN
- EIN GERÄT VERWENDEN
- PROBLEMBEHANDLUNG
- PC AUSSCHALTEN

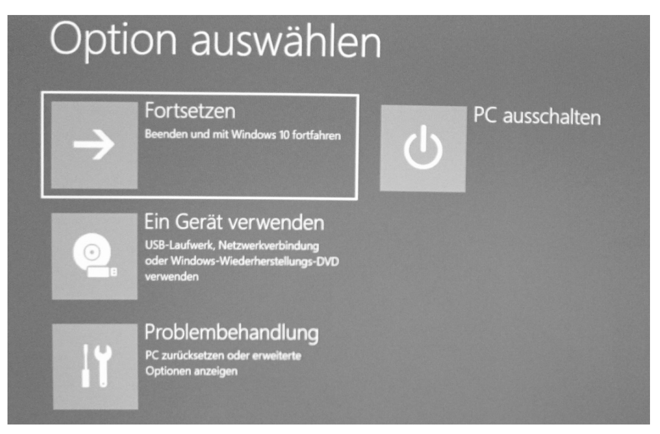


Abb. 16.7: Hauptbildschirm der Wiederherstellungsumgebung in Windows 10

Klicken Sie auf Problembehandlung, um weitere Optionen anzuzeigen. Windows 10 unterscheidet sich hier von früheren Versionen und vereint die Optionen PC AUFFRISCHEN und ORIGINALEINSTELLUNG WIEDERHERSTELLEN in einer Schaltfläche DIESEN PC ZURÜCKSETZEN. Windows 8.1 bietet beispielsweise drei Optionen (Abbildung 16.8):

- PC AUFFRISCHEN
- ORIGINALEINSTELLUNG WIEDERHERSTELLEN
- ERWEITERTE OPTIONEN



Abb. 16.8: Optionen der PROBLEMBEHANDLUNG in Windows 8.1

Das Verständnis der Optionen PC AUFFRISCHEN und ORIGINALEINSTELLUNG WIEDERHERSTELLEN ist bei der Fehlerbehebung und gegebenenfalls der Wiederherstellung eines PCs mit Windows 8/8.1/10 von entscheidender Bedeutung. Mehr dazu in Kürze.

Mit einem Klick auf ERWEITERTE OPTIONEN gelangen Sie zu einem weiteren Menü (Abbildung 16.9), das viele der aus Windows 7 bekannten Optionen bereithält:

- SYSTEM WIEDERHERSTELLEN
- SYSTEMIMAGE-WIEDERHERSTELLUNG
- STARTHILFE
- UPDATES DEINSTALLIEREN
- EINGABEAUFFORDERUNG
- UEFI-FIRMWAREEINSTELLUNGEN (nur verfügbar, wenn Ihr Mainboard UEFI statt des klassischen BIOS verwendet)



Abb. 16.9: Das Menü ERWEITERTE OPTIONEN in Windows 10

Wichtig

Sie sollten wissen, wie Sie auf die Windows-Wiederherstellungsumgebung zugreifen können und was die verschiedenen Werkzeuge leisten.

Jetzt betrachten wir die Optionen etwas eingehender, sowohl die aus Windows 7 bekannten als auch die beiden zusätzlichen Optionen in Windows 10, UPDATES DEINSTALLIEREN und UEFI-Firmware-einstellungen.

Systemstartreparatur Bei der Starthilfe/Systemstartreparatur (Abbildung 16.10) werden eine Reihe verschiedener Werkzeuge eingesetzt, unter anderem:

- Es findet die Reparatur einer beschädigten Registry durch Verwendung einer Sicherheitskopie auf der Festplatte statt.
- Unverzichtbare Bootdateien werden wiederhergestellt.
- Wichtige Systemdateien und Gerätetreiber werden wiederhergestellt.
- Rückkehr zu vorherigen Treibern, wenn diese nicht funktionieren (»Driver Rollback«)
- Updates werden deinstalliert.
- `chkdsk` wird ausgeführt.
- Die Speicherdiagnose zur Überprüfung des RAMs wird ausgeführt.

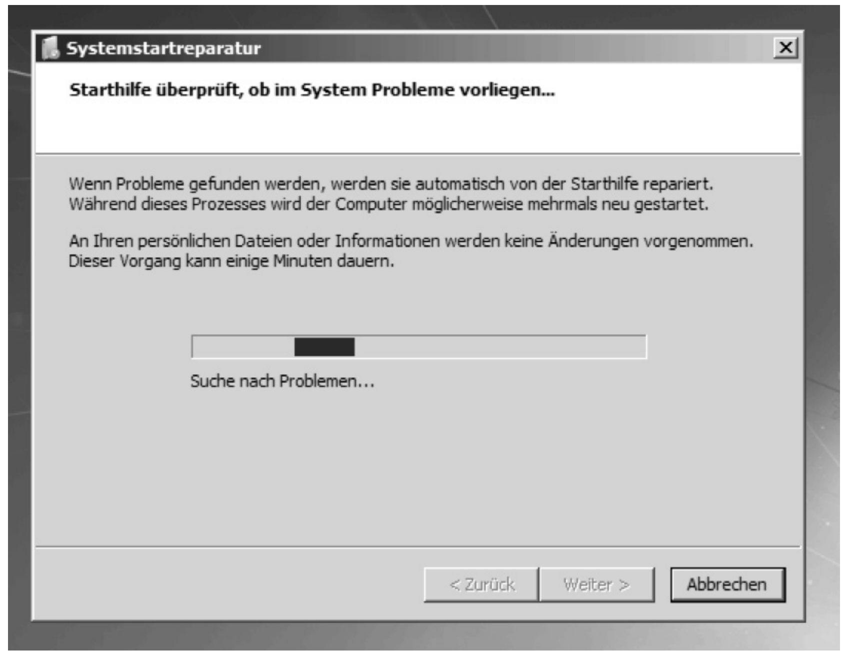


Abb. 16.10: Systemstartreparatur in Aktion

Die Systemstartreparatur kann fast alle Startprobleme beheben. Tatsächlich dürften Sie Schwierigkeiten haben, bei einem System mit einer einzelnen Festplatte und nur einer Partition mit Windows 7 ein Problem zu finden, das die Systemstartreparatur *nicht* beheben kann. Wenn das Werkzeug seine Arbeit erledigt hat, wird eine Meldung angezeigt (Abbildung 16.11).

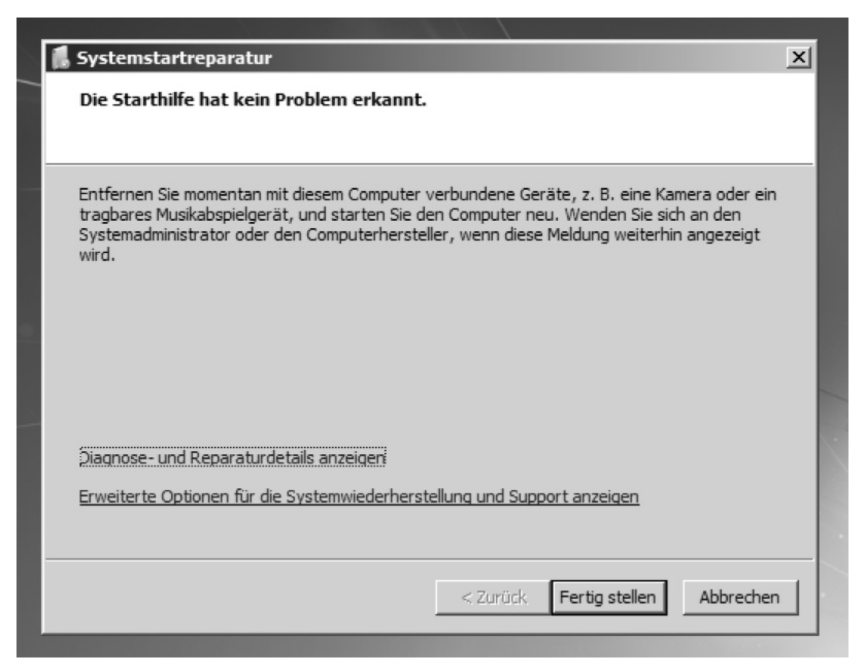


Abb. 16.11: Systemstartreparatur beendet, keine Probleme gefunden

Beachten Sie in Abbildung 16.11 den Link DIAGNOSE- UND REPARATURDETAILS ANZEIGEN. Wenn Sie ihm folgen, wird eine Textdatei namens `srttrail.txt` geöffnet, die genau aufführt, welche Probleme das Programm gefunden hat, welche Fehler repariert wurden und bei welchen Fehlern die Reparatur gescheitert ist. Die Meldungen sehen zwar kryptisch aus, aber eine Suche im Internet hilft oft schnell weiter. Ein kleiner Auszug der (sehr langen) Datei ist nachstehend wiedergegeben.

```
Startup Repair diagnosis and repair log
---------------------------
Last successful boot time: 2/14/2016 2:37:43 AM (GMT)
Number of repair attempts: 6

Session details
---------------------------
System Disk = \Device\Harddisk0
Windows directory = C:\Windows
AutoChk Run = 0
Number of root causes = 1
Test Performed:
---------------------------
Name: Check for updates
Result: Completed successfully. Error code = 0x0
Time taken = 32 ms
Test Performed:
---------------------------
Name: System disk test
Result: Completed successfully. Error code = 0x0
Time taken = 0 ms
```

Hinweis

Der Link ERWEITERTE OPTIONEN FÜR DIE SYSTEMWIEDERHERSTELLUNG UND SUPPORT ANZEIGEN führt Sie einfach nur zum Hauptbildschirm zurück.

In Windows 7 und neueren Windows-Versionen wird die Systemstartreparatur automatisch gestartet, wenn das System ein Startproblem erkennt. Wenn beim Einschalten ein Bildschirm wie in Abbildung 16.12 angezeigt wird, hat Windows beim Start ein Problem entdeckt.

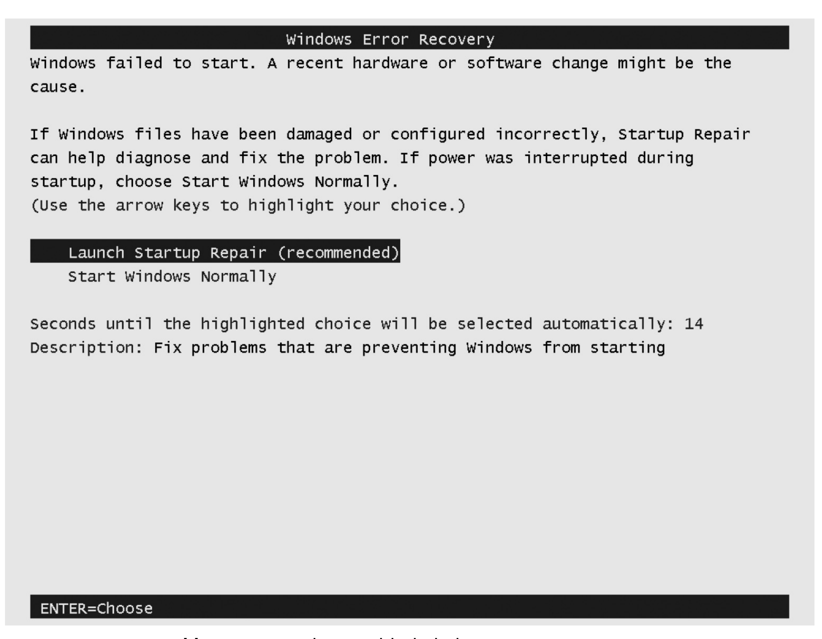


Abb. 16.12: Windows-Fehlerbehebung (Error Recovery)

Aber auch ein so leistungsfähiges Werkzeug wie die Systemstartreparatur stößt irgendwann einmal an seine Grenzen. Möglicherweise bestehen spezielle Anforderungen, die etwas Ausgefeilteres verlangen als den Ein-Programm-für-alles-Ansatz. Es kommt auch vor, dass man das eigentliche Problem bereits erkannt hat und nur eine einzige Reparatur durchführen möchte. Vielleicht beabsichtigen Sie auch, eine Systemwiederherstellung oder eine Speicherdiagnose auszuführen. Zu diesem Zweck müssen wir die anderen Optionen von WinRE untersuchen.

Wichtig

Wenn Sie beim Start des Computers auf Schwierigkeiten stoßen, sollten Sie als Erstes die Systemstartreparatur ausprobieren. Das trifft nicht nur zu, wenn das System nicht mehr bootet, sondern auch, wenn es sehr langsam startet.

Systemwiederherstellung Die Systemwiederherstellung erledigt dieselbe Aufgabe, seit Microsoft sie mit Windows Me eingeführt hat. Sie erlaubt es Ihnen, zu einem Zeitpunkt zurückzukehren, an dem Ihr System noch tadellos funktionierte. Das Vorhandensein dieser Option in Windows RE erlaubt denjenigen unter uns, die häufig Systemwiederherstellungspunkte (Momentaufnahmen des Systems zu einem bestimmten Zeitpunkt) erstellen, eine schnelle und einfache Rückkehr zu einem früheren Zustand des Systems (Abbildung 16.13).

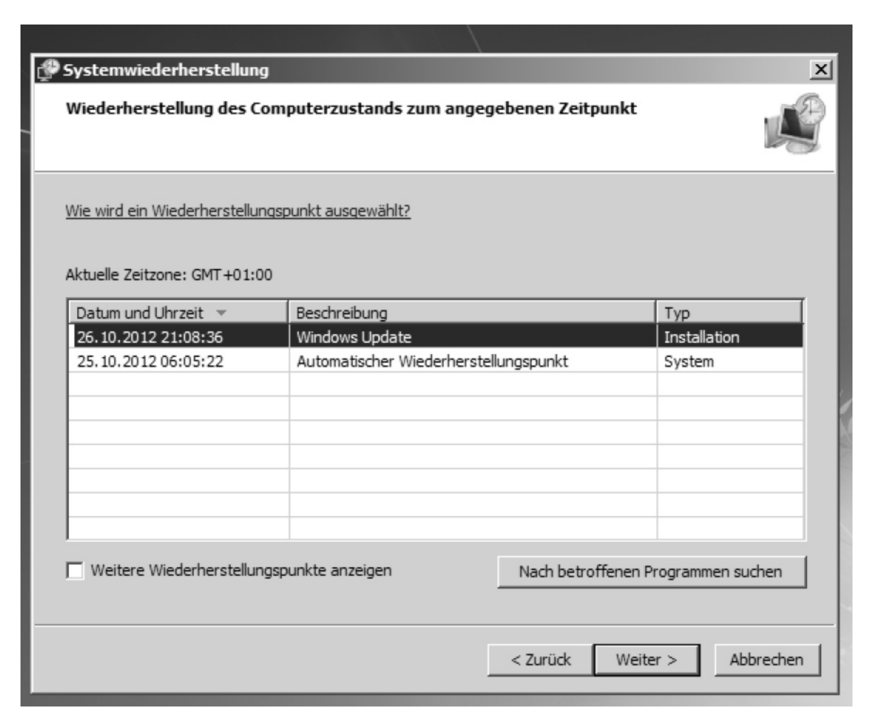


Abb. 16.13: Systemwiederherstellungspunkte

Hinweis

In Kapitel 14 wurde bereits erwähnt, dass die Systemwiederherstellung in Windows 10 standardmäßig deaktiviert ist. Wenn Sie also einen Rechner mit Windows 10 mit der Systemwiederherstellung reparieren wollen, besteht durchaus die Möglichkeit, dass Sie keine Wiederherstellungspunkte vorfinden.

Wichtig

macOS bietet ein erstaunlich mächtiges Werkzeug zum Beenden problematischer Anwendungen namens PROGRAMME SOFORT BEENDEN. Drücken Sie [⌘] + [Alt] + [ESC] um ein Fenster mit einer Liste der laufenden Programme anzuzeigen.

Systemabbild-Wiederherstellung Wenn Sie ein Systemabbild zur Hand haben, können Sie diese Funktion im Katastrophenfall zur Systemwiederherstellung einsetzen. Das erweist sich als äußerst praktisch, wenn man eine Reihe einheitlich konfigurierte Systeme verwaltet, wie es in vielen Umgebungen üblich ist. Halten Sie ein Systemabbild bereit, das die Einstellungen des Betriebssystems, des Netzwerks und die benötigten Anwendungen umfasst. Dann können Sie einen Computer, der im Eimer ist, schnell wieder zum Laufen bringen. Sie können zudem ein einfacheres Systemabbild erstellen, das nur das Betriebssystem enthält, das Sie dann konfigurieren können.

Wenn das Laufwerk mit dem Systemabbild angeschlossen ist, während Sie den Assistenten starten, sollte er Ihre letzte Sicherungskopie erkennen und Ihnen ein Dialogfeld wie in Abbildung 16.14 anzeigen. Falls ein falsches oder gar kein Systemabbild aufgeführt ist, können Sie auf der Festplatte oder sogar auf Netzwerkfreigaben nach anderen suchen.



Abb. 16.14: Auswahl eines Systemabbilds in Windows 7

Nach Auswahl des wiederherzustellenden Systemabbilds werden Ihnen weitere Optionen angeboten (Abbildung 16.15). Insbesondere können Sie auswählen, Festplatten zu formatieren und zu partitionieren. Wenn Sie sich für diese Option entscheiden, werden existierende Partitionen und Daten gelöscht und das wiederhergestellte System erhält dieselbe Partitionsstruktur wie das gesicherte System.



Abb. 16.15: Weitere Optionen bei der Systemwiederherstellung

Wenn Sie auf dem Bestätigungsbildschirm (Abbildung 16.16), der eine letzte Warnung anzeigt, FERTIGSTELLEN auswählen, beginnt der Wiederherstellungsvorgang (Abbildung 16.17). Das alte System wird entfernt und der Inhalt des gesicherten Systems wird auf die Festplatte(n) übertragen. Nach Abschluss der Wiederherstellung startet das System neu und Sie sollten es in dem Zustand vorfinden, in dem es sich zum Zeitpunkt der letzten Sicherung befand.

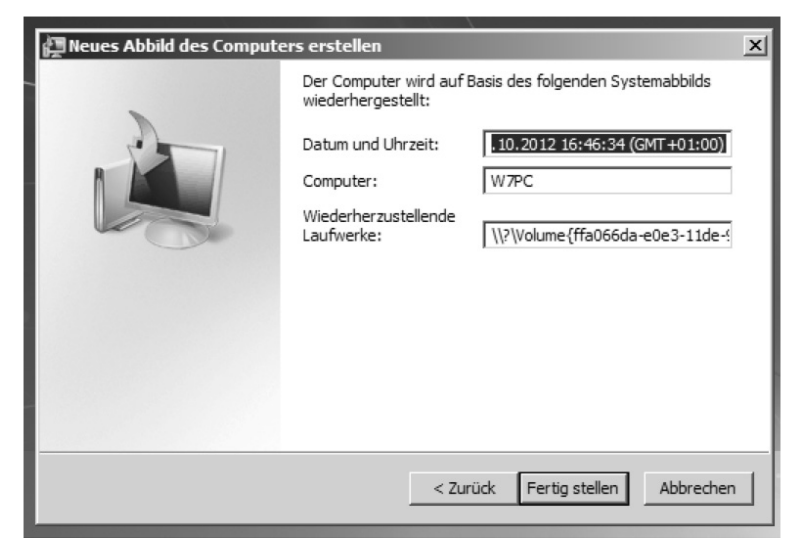


Abb. 16.16: Bestätigung der Einstellungen

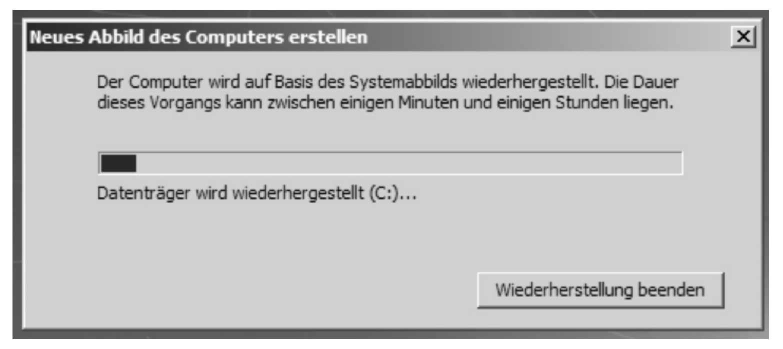


Abb. 16.17: Die Wiederherstellung ist in Arbeit.

Wenn Sie eine Systemabbild-Wiederherstellung in Windows 10, macOS oder Linux durchführen möchten, benötigen Sie Software eines Drittherstellers. Mir gefallen Acronis True Image für Windows und macOS und Clonezilla für Linux gut.

Windows-Speicherdiagnose Defekte RAM-Bausteine bereiten jedem Betriebssystem größte Probleme, die oft zu einem Blue Screen, »eingefrorenen« Systemen oder unvermittelten Neustarts führen. In Windows 7 können Sie im Hauptmenü von WinRE auf WINDOWS-SPEICHERDIAGNOSE klicken, und haben die Wahl zwischen JETZT NEU STARTEN UND NACH PROBLEMEN SUCHEN (EMPFOHLEN) und NACH PROBLEMEN BEIM NÄCHSTEN START DES COMPUTERS SUCHEN (Abbildung 16.18). Im Grunde genommen spielt es keine Rolle, welche der Optionen Sie auswählen, aber wenn Sie glauben, dass Ihre RAM-Bausteine überprüft werden sollten, bedeutet das vermutlich, dass Sie es sofort erledigen möchten.

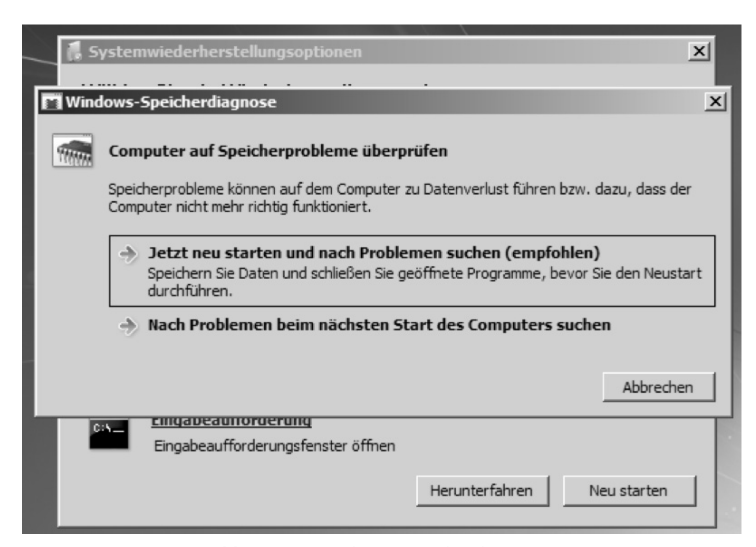


Abb. 16.18: Windows-Speicherdiagnose

Wichtig

In Windows 8/8.1/10 können Sie über die Systemsteuerung im Bereich VERWALTUNG auf die Speicherdiagnose zugreifen. Oder geben Sie in das Suchfeld der Taskleiste `Speicherdiagnose` ein. In diesen Windows-Versionen gibt es in WinRE die Option SPEICHERDIAGNOSE nicht. Nach dem Neustart sind die Schritte aber stets die gleichen.

Nach dem Neustart wird unmittelbar die Windows-Speicherdiagnose durchgeführt (Abbildung 16.19). Während das Programm läuft, können Sie jederzeit F1 drücken, um die Optionen der Speicherdiagnose anzuzeigen (Abbildung 16.20).

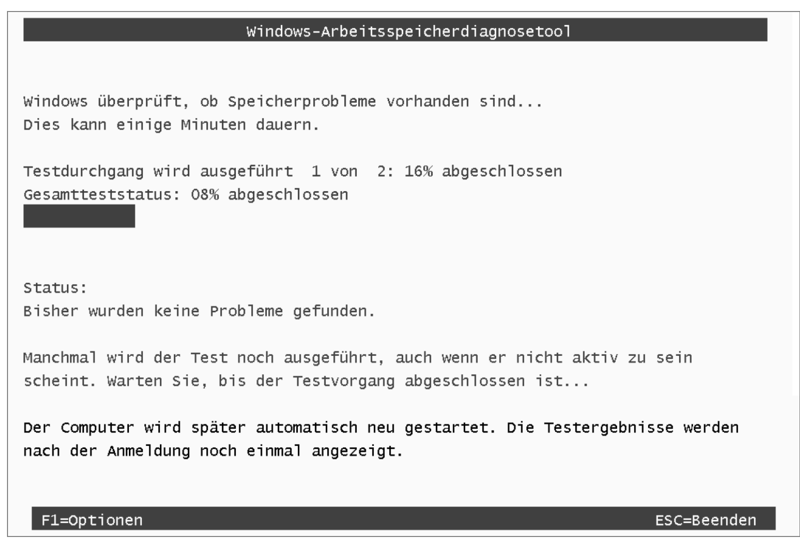


Abb. 16.19: Speicherdiagnose läuft ...



Abb. 16.20: Optionen der Speicherdiagnose

Am oberen Bildschirmrand werden drei verschiedene Tests angeboten: Minimal, Standard und Erweitert. Minimal ist zwar schnell (ca. 1 Minute), unterzieht den Arbeitsspeicher aber nur einfachen Tests. Standard, die Voreinstellung, dauert einige Minuten, testet den Speicher jedoch etwas aggressiver. Erweitert dauert stundenlang (lassen Sie den Test über Nacht laufen), testet Ihren Arbeitsspeicher aber auch wirklich auf Herz und Nieren.

Hinweis

Zur Windows-Speicherdiagnose gelangen Sie in der Systemsteuerung über System und Sicherheit|Verwaltung oder von der Eingabeaufforderung aus durch Eingabe des Kommandos `mdsched`.

Es gibt zwei weitere Optionen: Cache und Durchlaufanzahl. Die Option Cache erlaubt es Ihnen einzustellen, ob die Tests den eingebauten Cache-Speicher der CPU verwenden sollen, und ermöglicht das Überschreiben der vorgegebenen Cache-Einstellungen bei den verschiedenen Testarten. Belassen Sie es am besten bei der Voreinstellung. Die Durchlaufanzahl legt fest, wie oft die einzelnen Tests durchgeführt werden. Voreingestellt ist der Wert 2.

Wenn die Speicherdiagnose beendet ist, wird der Rechner neu gestartet. Das Resultat finden Sie in der Ereignisanzeige (Abbildung 16.21).

Leider haben mich die Ergebnisse der Windows-Speicherdiagnose nicht überzeugt. Hier im Testlabor von Total Seminars bewahren wir eine Menge fehlerbehaftete Speicherbausteine auf. Beim Testen haben wir es nicht geschafft, dem Werkzeug mehr als einen Blue Screen oder ein eingefrorenes System zu entlocken. Wir wenden uns wieder bewährten Tools wie dem kostenlosen Memtest86+ zu, wenn wir defekte RAM-Bausteine als Fehlerursache vermuten.

Hinweis

Wenn Sie sich für Memtest86+ interessieren, besuchen Sie `http://www.memtest.org`.

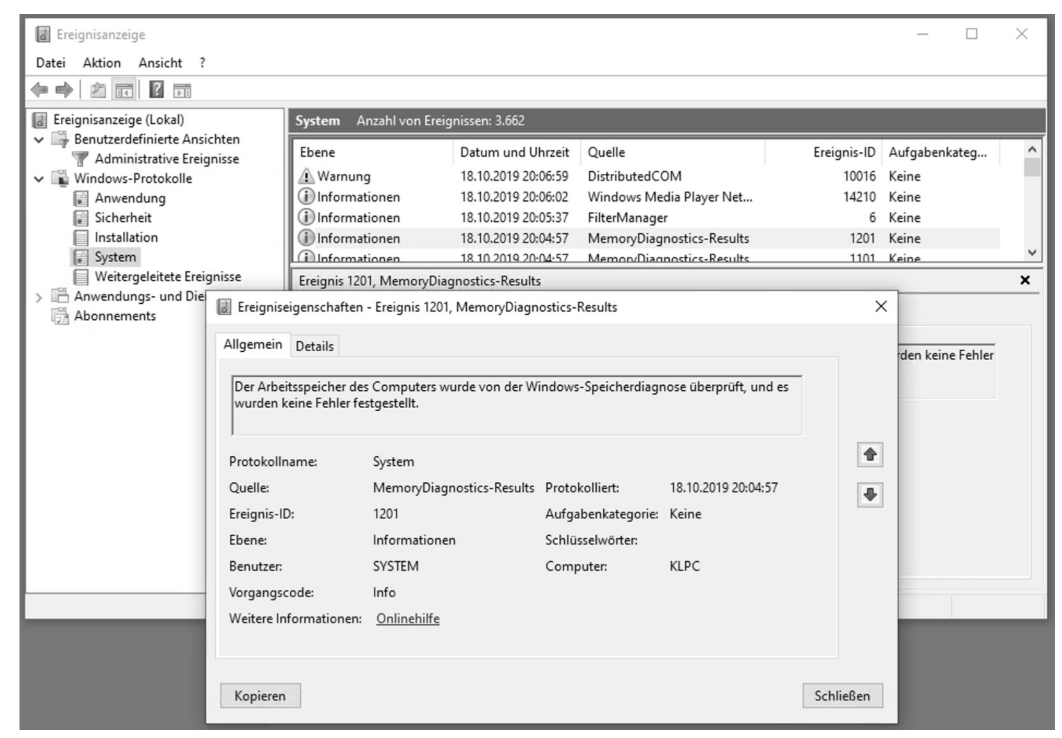


Abb. 16.21: Resultate der Speicherdiagnose

Eingabeaufforderung und bootrec Die letzte, interessanteste und zweifelsohne auch abgehobenste Option im WinRE-Menü ist die EINGABEAUFFORDERUNG. Hierbei handelt es sich um eine vollwertige 32-Bit- oder 64-Bit-Kommandozeile, die wie die normale Eingabeaufforderung funktioniert. Außerdem gibt es in der WinRE-Eingabeaufforderung ein wichtiges Werkzeug (`bootrec`), das in der normalen Kommandozeile nicht zur Verfügung steht. Zwar fehlen der WinRE-Eingabeaufforderung viele der sonst in der Eingabeaufforderung vorhandenen Kommandozeilenprogramme, die wichtigsten sind jedoch verfügbar. Lassen Sie uns zunächst das `bootrec`-Kommando untersuchen. Danach sehen wir uns noch einige andere Tools der WinRE-Eingabeaufforderung an.

Hinweis

Bei der Systemstartreparatur werden viele dieser Programme automatisch ausgeführt. Die WinRE-Eingabeaufforderung müssen Sie nur dann verwenden, wenn die Systemstartreparatur scheitert.

Es muss an dieser Stelle angemerkt werden, dass in den CompTIA A+-Prüfungen nicht von Ihnen erwartet wird, dass Sie alle Einzelheiten über diese Kommandozeilenprogramme kennen. Folgendes sollten Sie aber wissen:

- Welche Werkzeuge verfügbar sind und wie diese heißen
- Wie Sie auf diese Werkzeuge zugreifen können (insbesondere auf WinRE)
- Welche Aufgabe die Werkzeuge im Wesentlichen erfüllen
- Einige der grundlegenden Parameter/Schalter dieser Werkzeuge
- Wie Sie unter Anleitung, beispielsweise telefonisch durch einen Support-Mitarbeiter, diese Werkzeuge zur Reparatur von Computern verwenden können

Nachdem das klargestellt ist, können wir uns dem wohl wichtigsten Befehl der WinRE-Eingabeaufforderung widmen: `bootrec`.

Das `bootrec`-Kommando ist Bestandteil der Windows-Wiederherstellungsumgebung und dient der Reparatur des Master Boot Records, des Bootsektors oder des BCD-Stores (*Boot Configuration Data Store*). Es ersetzt die alten Programme `fixboot` und `fixmbr` der Wiederherstellungskonsole (ein Tool in Windows XP) und kennt noch zwei weitere Funktionen zur Reparatur:

- `bootrec /fixboot` Schreibt einen neuen Bootsektor auf die aktive Systempartition
- `bootrec /fixmbr` Schreibt einen neues Master Boot Record auf die Systempartition
- `bootrec /scanos` Sucht nach Windows-Installationen, die im BCD-Store noch nicht vorhanden sind, und zeigt das Resultat an, ohne irgendwelche Änderungen vorzunehmen
- `bootrec /rebuildmbr` Sucht nach Windows-Installationen, die im BCD-Store noch nicht vorhanden sind, und bietet Ihnen an, diese hinzuzufügen

Hinweis

Die BCD-Dateien enthalten Informationen über die auf dem Computer installierten Betriebssysteme. Im Microsoft-Jargon werden diese als *BCD-Store* bezeichnet.

Es gibt es ein Programm namens `bcdedit`, das Sie dazu verwenden können, sich den Start von Windows detailliert anzusehen. Der Aufruf von `bcdedit` (ohne Parameter) zeigt die Boot-Optionen an. Die nachstehenden Boot-Informationen entstammen einem System mit einer einzelnen Windows-Installation. Beachten Sie, dass es zwei Abschnitte gibt: Der Abschnitt *Windows Boot Manager* beschreibt den `bootmgr`-Speicherort und der Abschnitt *Windows Boot Loader* beschreibt den Speicherort der Datei `winload.exe`.

```
Windows Boot Manager
--------------------
identifier             {bootmgr}
device                  partition=\Device\HarddiskVolume1
descriptionWindows      Boot Manager
locale                  de-DE
inherit                 {globalsettings}
default                 {current}
resumeobject            {d4539c9b-481a-11df-a981-a17cb98be35c}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier            {current}
device                 partition=C:
path                   \Windows\system32\winload.exe
description            Windows 7
locale                 en-US
inherit                {bootloadersettings}
recoverysequence       {d4539c9d-481a-11df-a981-a17cb98be35c}
recoveryenabled        Yes
osdevice               partition=C:
systemroot             \Windows
resumeobject           {d4539c9b-481a-11df-a981-a17cb98be35c}
nx                     OptIn
```

Um Änderungen am BCD-Store vorzunehmen, müssen Sie die Schalter verwenden:

- `bcdedit /export <Dateiname>` Exportiert eine Kopie des BCD-Stores als Datei. Das sollten Sie auch bei jeder Verwendung von `bcdedit` tun!
- `bcdedit /import <Dateiname>` Liest eine Kopie des BCD-Stores wieder ein.

Wenn Sie sich die `bcdedit`-Ausgabe genauer ansehen, werden Sie bemerken, dass jeder Abschnitt am Anfang einen Bezeichner (`identifier`) wie `{bootmgr}` oder `{current}` besitzt. Sie können diese Bezeichner und den Schalter `/set` verwenden, um Änderungen am BCD-Store vorzunehmen. Hier ein Beispiel:

```
bcdedit /set {current} path \BackupWindows\system32\winload.exe
```

Hierdurch wird der Pfad (`path`) des Bezeichners `{current}` so geändert, dass er auf eine alternative `winload.exe`-Datei verweist.

Das `bcdedit`-Kommando unterstützt mehrere Betriebssysteme. Beachten Sie, dass der nachstehende BCD-Store drei Bezeichner besitzt: `{bootmgr}`, `{current}` und `{ntldr}`. Der letzte Bezeichner verweist auf ein sehr altes Betriebssystem, vermutlich Windows XP. Das bedeutet, dass der Computer sowohl das ältere Betriebssystem als auch Windows 7 booten kann.

```
Windows Boot Manager
--------------------
identifier              {bootmgr}
device                   partition=D:
description              Windows Boot Manager
locale                   de-De
inherit                  {globalsettings}
default                  {current}
resumeobject             {60b80a52-8267-11e0-ad8a-bdb414c1bf84}
displayorder             {ntldr}
                         {current}
toolsdisplayorder        {memdiag}
timeout                  30

Windows Legacy OS Loader
------------------------
identifier               {ntldr}
device                    partition=D:
path                      \ntldr
description               Ältere Windows-Version

Windows Boot Loader
-------------------
identifier               {current}

device                    partition=C:
path                      \Windows\system32\winload.exe
description               Windows 7
locale                    de-De
inherit                   {bootloadersettings}
recoverysequence          {60b80a54-8267-11e0-ad8a-bdb414c1bf84}
recoveryenabled           Yes
osdevice                  partition=C:
```

```
systemroot              \Windows
resumeobject            {60b80a52-8267-11e0-ad8a-bdb414c1bf84}
nx                      OptIn
```

Dieser BCD-Store würde beim Systemstart ein Boot-Menü wie in Abbildung 16.22 hervorbringen.

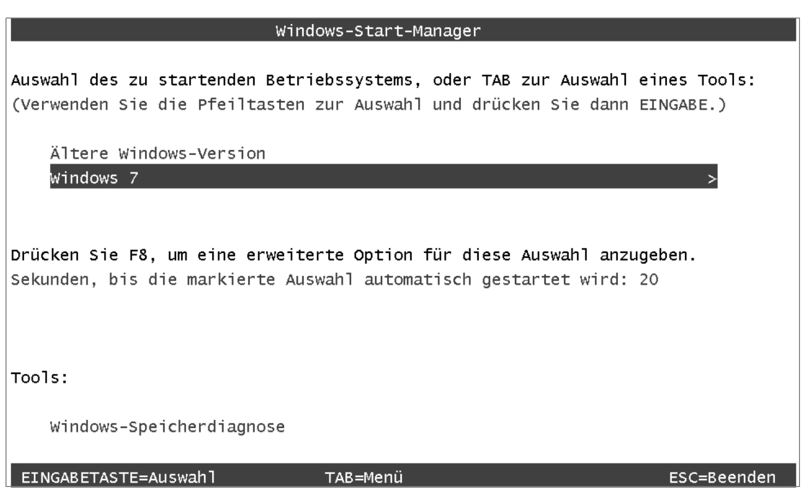


Abb. 16.22: Im Boot-Menü werden die verfügbaren Windows-Versionen angezeigt.

Sie können `bcdedit` verwenden, um die Optionen der Bootreihenfolge zu aktualisieren. Wenn Sie beispielsweise ein Multiboot-System wie das obige verwenden und feststellen, dass Sie häufig neu starten müssen, um eine Fehlerbehebung bei Programmen für eines der älteren installierten Betriebssysteme vorzunehmen, können Sie die Bootreihenfolge ändern, sodass standardmäßig das ältere Betriebssystem startet. Nachdem Sie den Fehler behoben haben, können Sie `bcdedit` verwenden, um die Bootreihenfolge wieder so zu ändern, dass standardmäßig Windows 10 startet.

In der Eingabeaufforderung steht darüber hinaus `diskpart` zur Verfügung, ein vollwertiges Partitionswerkzeug. Allerdings fehlen hier viele der Schutzfunktionen der Datenträgerverwaltung (siehe Kapitel 8), seien Sie also vorsichtig. Sie können beispielsweise jederzeit Partitionen jedes Typs löschen. Nach dem Start von `diskpart` erscheint eine spezielle Eingabeaufforderung:

```
C:\Windows\system32>diskpart
Microsoft DiskPart version 10.0.17134.345
Copyright (C) Microsoft Corporation.
On computer: MIKESPC
DISKPART>
```

Sie können sich eine Liste der Volumes (bzw. der Partitionen bei Basisfestplatten) ausgeben lassen:

```
DISKPART> list volume
Volume ### Ltr Label       Fs    Type       Size    Status    Info
---------- --- ----------- ----- ---------- ------- --------- --------
Volume 0    D                    DVD-ROM       0 B  No Media
Volume 1    C  New Volume  NTFS  Partition  1397 GB Healthy   System
DISKPART>
```

Wählen Sie ein Volume aus, an dem Sie Änderungen vornehmen möchten (Sie können auch die gesamte Festplatte auswählen):

```
DISKPART> select volume 1
Volume 1 is the selected volume.
DISKPART>
```

Sie können an der `diskpart`-Eingabeaufforderung Kommandos zum Hinzufügen, Ändern oder Löschen von Volumes und Partitionen ausführen, Volumes ein- und aushängen und sogar Software-basierte RAID-Verbunde steuern. Verwenden Sie den Befehl `format`, um neu erstellte Volumes zu formatieren.

Geben Sie auf der `diskpart`-Eingabeaufforderung den Befehl `clean` ein, um alle Partitionen und Volumes auf dem aktuell ausgewählten Laufwerk zu löschen. Dieses Werkzeug entfernt hartnäckige Fehler, die es verhindern, dass Windows bootet, und ist der letzte Strohhalm, nach dem ich greife, bevor ich ein Laufwerk wegwerfe.

Die auf der `diskpart`-Eingabeaufforderung verfügbaren Befehle können mit Volumes und Partitionen umgehen, Sie benötigen jedoch auch ein Werkzeug für Dateisysteme. Sowohl WinRE als auch die normale Eingabeaufforderung stellen die typischen Werkzeuge wie `copy`, `move`, `del` und `format` zur Verfügung. Ein weiteres Werkzeug namens `fsutil` kann allerdings noch ein paar andere interessante Aufgaben erledigen:

- Die Eingabe von `fsinfo` liefert ausführliche Informationen über die Laufwerke und Volumes.
- `fsutil dirty <Laufwerksname>` gibt darüber Auskunft, ob Windows das Laufwerk als »dirty« betrachtet. Wenn das der Fall ist, muss nach dem nächsten Neustart `autochk` ausgeführt werden. Wenn Windows im Dateisystem eines Laufwerks einen Fehler entdeckt, wird es als »dirty« markiert. Nach einem Neustart wird das Laufwerk noch vor dem Laden von Windows durch das Hilfsprogramm `autochk` überprüft, das die Fehler im Dateisystem behebt.
- Mit `fsutil repair initiate <Laufwerksbuchstabe>` wird eine vereinfachte Version von `chkdsk` (ohne Neustart) ausgeführt.

Updates deinstallieren Verwenden Sie diese Option, für den Fall, dass Microsoft ein Update veröffentlicht, das dafür sorgt, dass Ihr System nicht mehr richtig funktioniert. Das kam früher nur sehr selten vor, aber Microsoft bietet diese Option für den Fall der Fälle an. Sie werden Sie hoffentlich nie brauchen.

UEFI-Firmwareeinstellungen In die Firmwareeinstellungen von UEFI-basierten Mainboards zu gelangen, kann eine echte Herausforderung sein. Manchmal funktioniert das mehrmalige Betätigen der Taste `Entf` beim Start des Systems, aber die Gelegenheit dazu ist nur kurz. Diese Einstellungen ermöglichen es Ihnen, auf das Setup-Programm zuzugreifen, wenn Sie Ihr System über die Option WIEDERHERSTELLEN in den Einstellungen neu starten. Greifen Sie auf diese Option zurück, wenn Sie Änderungen an der Taktung von CPU und RAM vornehmen oder aus irgendeinem Grund die Bootreihenfolge ändern möchten.

PC auffrischen und zurücksetzen In Windows 8/8.1 gibt es auf dem Bildschirm PROBLEMBEHANDLUNG zwei Optionen, nämlich PC AUFFRISCHEN und ORIGINALEINSTELLUNG WIEDERHERSTELLEN. Windows 10 bietet die gleichen Optionen, die allerdings anders benannt sind. Sie sind unter DIESEN PC ZURÜCKSETZEN zu finden:

- *Auffrischen* in Windows 8/8.1 bedeutet in Windows 10 *kein Dateiverlust.*
- *Originaleinstellung wiederherstellen* in Windows 8/8.1 bedeutet in Windows 10 *alle Dateien entfernen.*

Die Ergebnisse der beiden Optionen unterscheiden sich natürlich drastisch.

Die in der Wiederherstellungsumgebung von Windows 8/8.1 verfügbare Option PC AUFFRISCHEN richtet Windows neu ein, erhält jedoch alle Benutzerdaten und Einstellungen sowie alle im Windows

Store erworbenen Anwendungen. Aber Achtung: *Alle anderen Anwendungen auf Ihrem System werden beim Auffrischen gelöscht!*

Die Option ORIGINALEINSTELLUNG WIEDERHERSTELLEN setzt Ihr System vollständig zurück – alle Apps, Programme, Benutzerdaten und Benutzereinstellungen werden gelöscht. Nach der Auswahl dieser Option finden Sie ein frisch installiertes Windows vor. Sie sollten sie bei der Fehlerbehebung nur als allerletzten Ausweg benutzen. Und vergessen Sie nicht, vorher eine Datensicherung durchzuführen.

16.1.2 Linux

Unter Linux sind zwei Boot-Manager gebräuchlich: GRUB und LILO. Heutzutage wird fast nur noch GRUB verwendet, denn das ältere LILO ist einfacher und unterstützt keine Systeme mit UEFI-BIOS.

Sollte GRUB beschädigt oder gelöscht worden sein, startet Linux nicht und es wird die Meldung `Missing GRUB` oder `GRUB nicht vorhanden` angezeigt. Auf älteren Systemen liefert LILO eine ähnliche Fehlermeldung.

Es gibt verschiedene Möglichkeiten, das Problem zu beheben. Wenn das System GRUB2 verwendet, können Sie von einem Installationsmedium starten und das System im Arbeitsspeicher »installieren« (nicht auf der Festplatte). Dann haben Sie Zugriff auf das Terminal und können den Befehl `sudo grub-install` ausführen, bei dem Sie das Startlaufwerk angeben müssen, das repariert werden soll.

16.2 Die grafische Benutzeroberfläche (GUI) startet nicht

Angenommen, Windows schafft es, während des Startprozesses zu booten, und fängt dann an, das grafische Windows-Betriebssystem zu laden. Sie sehen das Startbild auf dem Bildschirm, bis der Anmeldebildschirm erscheint (Abbildung 16.23). Nach der Anmeldung wird dann, je nach Windows-Version, der Desktop oder der Startbildschirm angezeigt.

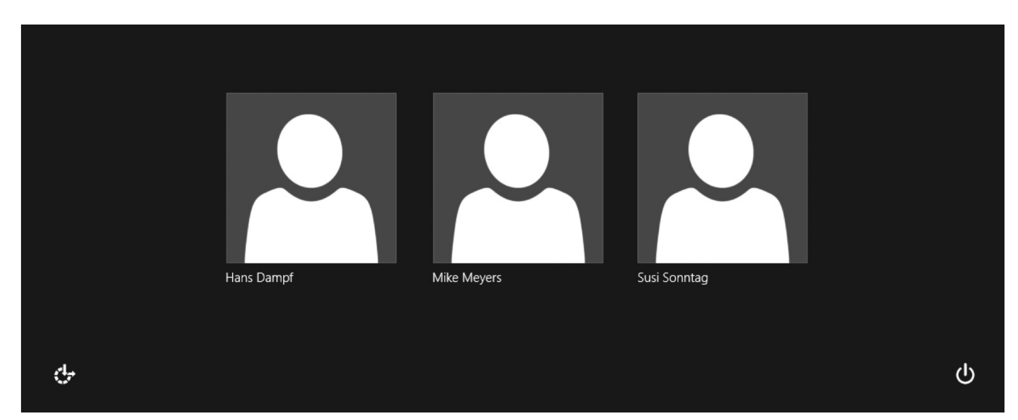


Abb. 16.23: Anmeldebildschirm

Es kann verschiedene Ursachen haben, wenn Windows die grafische Benutzeroberfläche nicht laden kann, wie beispielsweise fehlerhafte Treiber oder Probleme mit dem Registry. Selbst automatisch geladene Programme können dazu führen, dass die grafische Benutzeroberfläche nicht geladen werden kann. Und auch ein defektes Benutzerprofil kann eine normale Anmeldung verhindern. Der erste Schritt bei der Fehlersuche ist es, eine der erweiterten Startoptionen (wie später in diesem Kapitel beschrieben) zu verwenden, um diesen Punkt zu überwinden und Windows vollständig zu starten.

Wichtig

Wenn Sie einer Situation gegenüberstehen, in der die Anmeldung nicht funktioniert, starten Sie den Computer neu. Das ist die einfachste Möglichkeit, also probieren Sie sie aus!

16.2.1 Gerätetreiber

Wenn Probleme mit Gerätetreibern verhindern, dass die grafische Benutzeroberfläche geladen wird, können die Fehlermeldungen schon einigermaßen beängstigend wirken. Abbildung 16.24 zeigt den gefürchteten Stopp-Fehler von Windows, der auch *Blue Screen of Death* (BSoD) genannt wird. Der BSoD erscheint nur, wenn ein Fehler aufgetreten ist, den Windows nicht selbst beheben kann. Der BSoD wird zwar nicht nur bei Gerätetreiberproblemen angezeigt, diese sind aber eine der möglichen Ursachen.

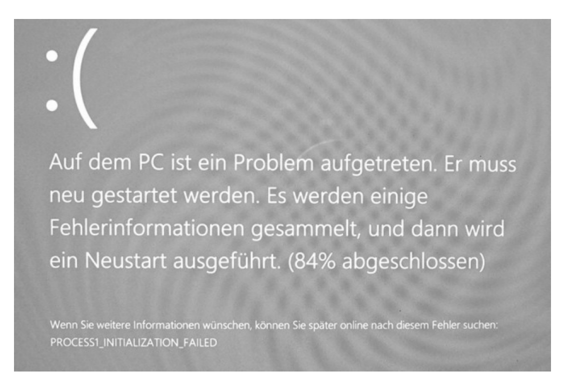


Abb. 16.24: Blue Screen in Windows 8.1

Immer wenn ein BSoD angezeigt wird, sollten Sie die angezeigten Fehlerinformationen lesen. Auf dem BSoD teilt Ihnen Windows den Namen der Datei mit, bei der ein Fehler aufgetreten ist, und schlägt Ihnen normalerweise auch geeignete Maßnahmen vor. Manchmal sind diese Hinweise hilfreich, oft aber auch nicht.

BSoD-Probleme aufgrund von Gerätetreibern treten fast immer unmittelbar nach der Installation eines neuen Geräts und dem Neustart des Computers auf. Bauen Sie das Gerät wieder aus und starten Sie den Rechner neu. Wenn Windows korrekt startet, suchen Sie die Website des Herstellers auf. Wenn ein neues Gerät diesen Fehler verursacht, liegt wirklich ein ernsthaftes Problem vor, das vor dessen Veröffentlichung hätte gelöst werden sollen. Häufig stellen die Hersteller aktualisierte Treiber zum Download bereit oder empfehlen einen Ersatztreiber.

Fehlerhafte Treiber für Grafikkarten können die Ursache dafür sein, dass Ihnen nur ein schwarzer Bildschirm im Textmodus angezeigt wird, der Hinweise auf den aufgetretenen Fehler und dessen Behebung enthält.

Wichtig

Auch Viren können die Ursache dafür sein, dass Windows nicht ordnungsgemäß startet oder dass es zumindest so erscheint. Kürzlich machte ein Virus die Runde, das einen gefälschten Blue Screen anzeigte, der vor einem unmittelbar bevorstehenden Ausfall des Festplatten-Controllers warnte. Selbst nachdem das Virus entfernt worden war, zeigte Windows keine Elemente der grafischen Benutzeroberfläche an: keine Schaltflächen, keine Icons, keine Dateien, nichts. Das Virus hatte die Attribute sämtlicher Dateien und Ordner geändert und auf VERSTECKT gesetzt. In Kapitel 27, *Computersicherheit*, werden wir uns damit befassen, wie man von Viren heimgesuchte PCs wieder in Ordnung bringt.

Beim zweiten Hinweis auf ein Geräteproblem, das während der GUI-Phase des Startprozesses auftritt, friert der Rechner ein: Der Windows-Startbildschirm wird angezeigt und bleibt einfach auf dem Bildschirm stehen, ohne dass Sie je die Möglichkeit zur Anmeldung bekommen. In solchen Fällen benutzen Sie eine der nachfolgend beschriebenen erweiterten Startoptionen.

Gerätetreiber können auch auf Linux-Systemen Probleme bereiten und eine eigene Art von BSoD auslösen, eine sogenannte Kernel Panic. Das Problem lässt sich auf die gleiche Weise wie unter Windows beheben: Besuchen Sie die Website des Herstellers und suchen Sie nach neuen Treibern oder Kernel-Erweiterungen (Code, der direkt dem Kernel hinzugefügt wird).

Fehlerhafte Hardware kann sowohl in macOS als auch Linux eine Kernel Panic verursachen. In macOS wird das durch einen schwarzen oder grauen Bildschirm signalisiert. Kein schöner Anblick, das kann ich Ihnen versichern.

Wichtig

Das *Pinwheel of Death*, das unter bestimmten Umständen in macOS angezeigt wird, weist normalerweise auf eine *einzelne* Anwendung hin, die nicht mehr reagiert. Es wird häufig mit dem BSoD und einer Kernel Panic in einen Topf geworfen, tatsächlich ist es für gewöhnlich nicht annähernd so schlimm.

16.2.2 Registry

Ihre Registry-Dateien werden bei jedem Start des Computers geladen. Windows schützt Ihre Registry-Dateien zwar ganz gut, aber manchmal übersieht auch Windows etwas und versucht dann, eine beschädigte Registry zu laden. Diese Fehler können zu einem BSoD führen, der auf einen Fehler mit der Registry-Datei hinweist, es können aber auch nur Textmeldungen angezeigt werden, die Ihnen mitteilen, dass Windows nicht gestartet werden kann. Unabhängig von der Ursache müssen Sie wieder für eine fehlerfreie Kopie der Registry sorgen. Am besten verwenden Sie dazu die Option LETZTE ALS FUNKTIONIEREND BEKANNTE KONFIGURATION, die im nächsten Abschnitt beschrieben wird. Wenn dies nicht funktioniert, können Sie über Windows RE eine ältere Version der Registry wiederherstellen.Windows 8.1 und frühere Versionen (und die ersten Versionen von Windows 10) erstellen regelmäßig Sicherungskopien der Registry. Das ist praktisch, wenn Sie eine beschädigte Registry ersetzen müssen. Standardmäßig wird diese Sicherung alle zehn Tage durchgeführt, es gehen Ihnen also schlimmstenfalls die Einträge der letzten zehn Tage verloren, wenn Sie die beschädigte Registry durch die automatisch erstellte Sicherungskopie ersetzen. Noch besser wäre es natürlich, wenn Sie selbst regelmäßig Sicherungskopien anlegen, aber auch so hält sich der Schaden in Grenzen. Die Sicherungskopie befindet sich im Verzeichnis `\Windows\System32\config\RegBack` (Abbildung 16.25).

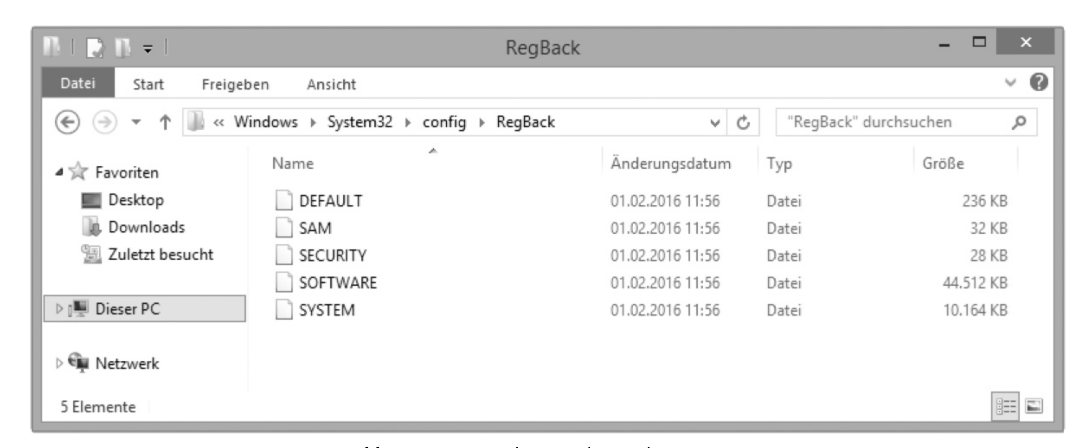


Abb. 16.25: Die Sicherungskopie der Registry

Zum Ersetzen der Registry müssen Sie von den Installations-Medien booten und WinRE verwenden. Öffnen Sie dort die Eingabeaufforderung und geben Sie dann das Kommando `reg` ein. Sie erhalten eine weitere Eingabeaufforderung, auf der Ihnen eine Vielzahl von Befehlen zum Bearbeiten der Registry zur Verfügung steht. Es ist wohl das Einfachste, das Kommando `copy` zu verwenden. Der Speicherort der Sicherungskopien ist Ihnen bereits bekannt. Kopieren Sie die Dateien an den Speicherort der Registry (eine Ebene höher im Verzeichnisbaum im Ordner `config`).

16.2.3 Erweiterte Startoptionen

Wenn Windows nicht mehr startet, stehen Ihnen je nach Betriebssystemversion verschiedene Optionen zur Verfügung. In Windows 7 sollten Sie beim Booten F5 drücken, um im abgesicherten Modus zu starten. Sie können sich auch über das Menü mit den *erweiterten Startoptionen* auf die Fehlersuche begeben. Dieses Menü wird angezeigt, wenn Sie den Computer neu starten und nach den BIOS-Meldungen, aber noch vor der Anzeige des Windows-Logos F8 drücken.

In Windows 8 und neueren Versionen können Sie zu den erweiterten Startoptionen gelangen, indem Sie einen »harten« Reset (Kaltstart) ausführen, wenn Windows abstürzt oder plötzlich neu startet. Früher oder später stellt das System fest, dass ein Problem vorliegt, und startet eine Diagnose. Sollte der Test scheitern, werden Ihnen die erweiterten Startoptionen angeboten. Eine genaue Beschreibung der Schritte und Bildschirmfotos von Microsoft finden Sie hier:

`https://support.microsoft.com/de-de/help/12376/windows-10-start-your-pc-in-safe-mode`

Abgesicherter Modus

Der *abgesicherte Modus* startet Windows, lädt aber nur die grundlegenden, nicht herstellerspezifischen Treiber für Maus, Monitor (in Windows 7 mit 800 x 600 Auflösung und in 8/8.1/10 mit 1024 x 768 Auflösung), Tastatur, Massenspeicher und Systemdienste (Abbildung 16.26).



Abb. 16.26: Abgesicherter Modus

Sobald Sie sich im abgesicherten Modus befinden, können Sie mit Tools wie dem Geräte-Manager nach der Ursache des Fehlers forschen und ihn zu beheben versuchen. Wenn Sie den Geräte-Manager im abgesicherten Modus verwenden, können Sie auf alle Eigenschaften der Geräte zugreifen, und zwar auch bei denen, die im abgesicherten Modus nicht funktionieren. Der für das jeweilige Gerät angezeigte Status entspricht dem Status beim normalen Start. Selbst Netzwerkkarten werden in diesem Modus als aktiviert angezeigt. Verdächtige Geräte können Sie nun deaktivieren. Auch andere Aufgaben wie das Entfernen oder Aktualisieren von Treibern können durchgeführt werden. Falls Probleme mit einem Gerätetreiber auftreten, die den normalen Start des Betriebssystems verhindern, können Sie an dieser Stelle nach den Warnsymbolen Ausschau halten, die unbekannte Geräte kennzeichnen.

Es gibt in keiner Windows-Version eine Schutz- oder Reparaturfunktion, die dafür sorgt, dass Windows automatisch im abgesicherten Modus startet. Wenn Windows dennoch automatisch im abgesicherten Modus startet, hat meistens jemand mit dem Systemkonfigurationsprogramm das so eingerichtet. Wählen Sie START|SUCHEN oder START|AUSFÜHREN, geben Sie `msconfig` ein und drücken Sie [↵], um das Systemkonfigurationsprogramm zu öffnen. Hier können Sie das entsprechende Kontrollkästchen deaktivieren (Abbildung 16.27).

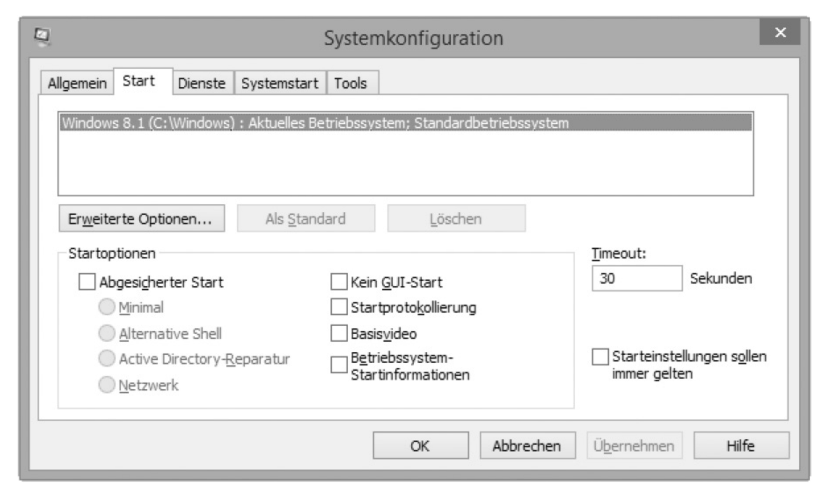


Abb. 16.27: Abgesicherten Start deaktivieren

Abgesicherter Modus mit Netzwerktreibern

Dieser Modus entspricht dem einfachen abgesicherten Modus, nur dass hier die Netzwerkunterstützung geladen wird. Ich verwende diesen Modus bei Problemen mit Netzwerktreibern. Falls Windows nicht normal starten kann, es aber im abgesicherten Modus tut, kann ich in den abgesicherten Modus mit Netzwerktreibern starten. Ist der Start mit Netzwerktreibern nicht möglich, dann liegt das Problem bei einem Netzwerktreiber. Ich starte dann erneut im abgesicherten Modus, führe den Geräte-Manager aus und beginne dann mit dem Deaktivieren der Netzwerkkomponenten, wobei ich zunächst den Netzwerkadapter selbst deaktiviere.

Abgesicherter Modus mit Eingabeaufforderung

Wenn Sie Windows in diesem Modus starten und nicht den Desktop im grafischen Modus laden, wird nach der Anmeldung die Eingabeaufforderung (`cmd.exe`) als Benutzeroberfläche des Betriebssystems angezeigt. Von hier aus können Sie alle Kommandos, die Sie in Kapitel 15 kennengelernt haben, und weitere Werkzeuge verwenden. Sie können beispielsweise `chkdsk` zur Fehlerüberprüfung ausführen. Die Defragmentierung läuft sogar ein klein wenig schneller als unter der grafischen Benutzeroberfläche, wenn Sie `defrag` gefolgt von einem Leerzeichen und einem Laufwerksbuchstaben eingeben.

Wichtig

In den Lernzielen der CompTIA wird eine Situation erwähnt, in der es darum geht, eine Festplatte (HDD) zu defragmentieren, um Probleme mit Windows zu lösen. Das ist mit der Eingabeaufforderung im abgesicherten Modus problemlos möglich.

Der abgesicherte Modus mit Eingabeaufforderung ist auch praktisch, wenn der Desktop überhaupt nicht mehr angezeigt wird. Wenn Fehler der Grafikkartentreiber auszuschließen sind, kann dieser Fall eintreten, wenn das Programm `explorer.exe` beschädigt ist. An der Eingabeaufforderung können Sie dann die beschädigte Datei `explorer.exe` durch eine intakte Version ersetzen. Dazu müssen Sie allerdings mit der Arbeit und den Befehlen zum Navigieren innerhalb der Verzeichnisstruktur auf der Kommandozeile vertraut sein. Außerdem müssen Sie den Speicherort der zu ersetzenden Dateien kennen. Auch wenn der Explorer selbst nicht geladen wird, können Sie immer noch andere GUI-Tools laden, die nicht vom Explorer abhängen. Sie müssen dazu lediglich den richtigen Befehl eingeben. Zum Start der Ereignisanzeige geben Sie beispielsweise in der Befehlszeile `eventvwr.msc` ein und drücken ↵.

Startprotokollierung aktivieren

Diese Option startet Windows normal und erzeugt dabei eine Protokolldatei mit den Namen der in den Speicher geladenen Treiber. Die Datei heißt `Ntbtlog.txt` und wird im Ordner `%SystemRoot%` gespeichert. Falls der Start wegen eines fehlerhaften Treibers fehlschlägt, verweist der letzte Eintrag in dieser Datei auf den Treiber, der beim Auftreten des Fehlers vom Betriebssystem zuletzt initialisiert wurde.

Starten Sie den Rechner neu und rufen Sie die Wiederherstellungsumgebung auf. Benutzen Sie die verfügbaren Befehle, um das Startprotokoll zu lesen, und zum Deaktivieren oder Aktivieren problematischer Geräte oder Dienste.

Anzeige mit niedriger Auflösung aktivieren

ANZEIGE MIT NIEDRIGER AUFLÖSUNG AKTIVIEREN startet Windows normal, lädt aber nur einen Standardtreiber. Wenn dieser Modus funktioniert, wissen Sie, dass Sie einen fehlerhaften Grafikkartentreiber verwenden oder dass der Grafiktreiber zwar korrekt ist, aber falsch konfiguriert wurde (möglicherweise ist die Bildwiederholrate und/oder die Auflösung falsch). Nach dem Start in diesem Modus öffnen Sie die Anzeigeeigenschaften und ändern die Einstellungen.

Letzte als funktionierend bekannte Konfiguration

Falls Windows gleich nach der Installation eines neuen Treibers, aber noch vor der erneuten Anmeldung beim System hängt, können Sie die Option LETZTE ALS FUNKTIONIEREND BEKANNTE KONFIGURATION ausprobieren. Diese Option ist insbesondere dann anzuwenden, wenn neue Gerätetreiber dazu führen, dass der Systemstart fehlschlägt.

Verzeichnisdienstwiederherstellung

Die Bezeichnung weist bereits darauf hin, dass sich diese Option auf Domänen-Controller für Active Directory bezieht. Diese Rolle können nur Windows-Server-Versionen übernehmen, weshalb ich nicht weiß, warum Microsoft die Option überhaupt mit aufgenommen hat. Wenn Sie diese bei den anderen Windows-Versionen auswählen, bootet der Rechner einfach im abgesicherten Modus.

Debugmodus

Wenn Sie diese Option auswählen, startet Windows im Kernel-Debugmodus. Die Sache ist derart technisch, dass wahrscheinlich selbst Supertechniker diesen Modus heute nicht mehr benutzen. Sie müssen den Computer dazu über eine serielle Verbindung mit einem anderen Computer verbinden.

Beim Start von Windows wird ein Speicherabbild des Kernels an den zweiten Computer gesendet, auf dem ein entsprechendes Debuggerprogramm laufen muss.

Automatischen Neustart bei Systemfehlern deaktivieren

Manchmal erscheint beim Starten ein BSoD, und Ihr Computer startet sofort wieder neu. Das ist schön und gut, passiert aber manchmal so schnell, dass Sie gar nicht lesen können, wo die Ursache des Problems liegt. Wenn Sie den automatischen Neustart bei Systemfehlern über das Menü mit den erweiterten Startoptionen deaktivieren, unterbinden Sie den erneuten Start des Computers bei Stop-Fehlern. Dann können Sie sich die Informationen zum Fehler notieren und diesen hoffentlich leichter beheben.

Erzwingen der Treibersignatur deaktivieren

Unter Windows müssen alle wirklich systemnahen Treiber (die im Kernel-Modus ausgeführt werden) normalerweise von Microsoft signiert sein. Wenn Sie einen älteren Treiber verwenden, um einen Festplatten-Controller oder eine andere systemnahe Funktion nutzen zu wollen, dann müssen Sie diese Option benutzen, um Windows zum Laden des Treibers zu bewegen. Sie sollten aber besser immer prüfen, ob Ihr Mainboard und Ihre Festplatten mit Windows kompatibel sind und diese Option besser niemals benutzen.

Windows normal starten

Mit dieser Option wird Windows normal gestartet, ohne dass der Rechner neu gebootet wird. Sie haben ihn ja bereits neu gestartet, um zu diesem Menü zu gelangen. Dies ist die Option der Wahl, wenn Sie es sich anders überlegt haben und die übrigen exotischen Optionen doch nicht verwenden wollen.

Neu starten

Diese Option führt einen Warmstart des Rechners durch.

Zum Betriebssystemauswahlmenü zurückkehren

Auf Rechnern mit mehreren installierten Betriebssystemen führt Sie diese Option zum Betriebssystemauswahlmenü zurück, in dem Sie das zu ladende Betriebssystem auswählen können. Wenn Sie Windows 7 laden und [F8] drücken, um in das Menü mit den erweiterten Startoptionen zu gelangen, wird diese Option auch angezeigt.

16.2.4 Windows-Benutzerprofile wiederherstellen

Zu jedem Benutzerkonto auf einem Windows-Rechner gehört ein *Profil*, das Einstellungen enthält, wie Farben und Hintergrund des Desktops, Verknüpfungen oder andere Icons. Ein beschädigtes Profil kann die Anmeldung eines Benutzers und damit den Zugriff auf dessen Daten verhindern. Beschädigte Profile sind manchmal an sehr langen Ladezeiten erkennbar. Auch Anti-Schadsoftware kann unter Umständen ein Profil beschädigen, ebenso wie ein Upgrade einer Windows-Version. Sie haben zwei Möglichkeiten, ein beschädigtes Benutzerprofil zu reparieren. Entweder bearbeiten Sie eine Reihe von Einträgen in der Registry oder Sie legen ein neues Benutzerkonto an und kopieren die Einstellungen des Benutzers in das neue Benutzerkonto.

Die Bearbeitung der Registry ist ziemlich komplex, deshalb zeige ich die erforderlichen Schritte. Zunächst einmal müssen Sie sich im abgesicherten Modus befinden.

Wenn der Anmeldebildschirm angezeigt wird, Sie sich aber nicht anmelden können, ist es am einfachsten, die [⇧]-Taste gedrückt zu halten und dann EIN/AUS|NEU STARTEN auszuwählen, um in den abgesicherten Modus zu gelangen. Ihr Computer startet neu und Ihnen wird ein Bildschirm mit Optionen angezeigt, wie vorhin beschrieben. Wählen Sie PROBLEMBEHANDLUNG|ERWEITERTE OPTIO-

nen|Starteinstellungen aus und klicken Sie auf Neu starten. Nach kurzer Zeit werden die Starteinstellungen angezeigt, wo Sie den abgesicherten Modus (und anderes) auswählen können.

Sobald Sie sich im abgesicherten Modus befinden, benötigen Sie eine Eingabeaufforderung mit erhöhten Rechten. (Geben Sie im Suchfeld `cmd` ein, klicken Sie mit der rechten Maustaste auf die Eingabeaufforderung und wählen Sie Als Administrator ausführen aus.) Geben Sie `regedit` ein und drücken Sie ↵, um den Registrierungs-Editor zu öffnen. Navigieren Sie zu folgendem String, um eine Ansicht wie in Abbildung 16.28 zu erhalten:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
```

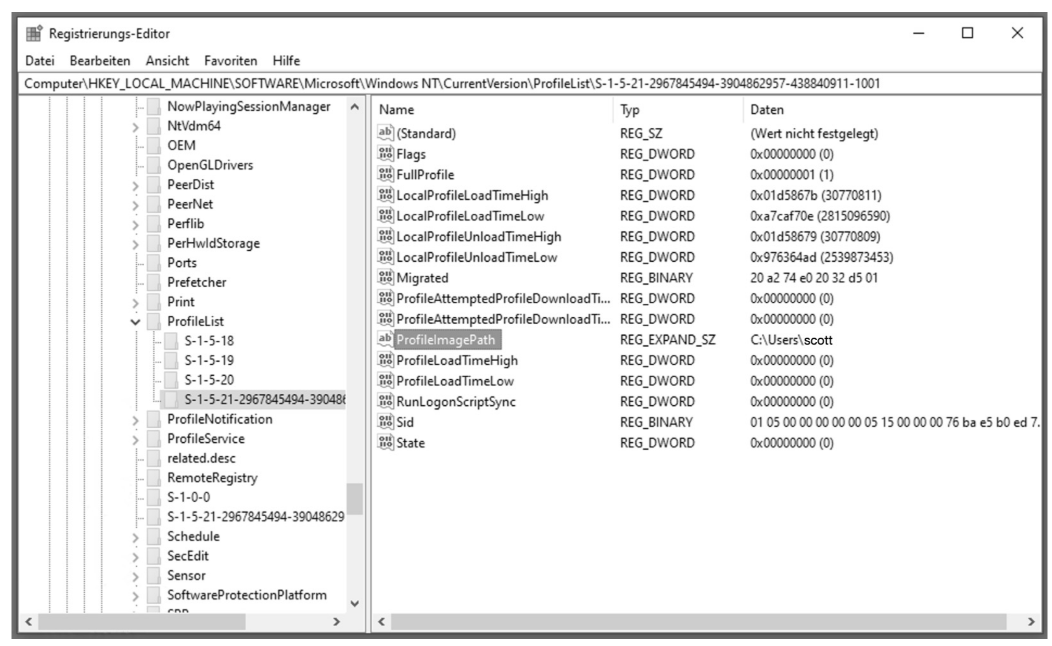


Abb. 16.28: Liste der Benutzerprofile im Registrierungs-Editor

Klicken Sie auf das Symbol links neben ProfileList, um eine Reihe von Einträgen anzuzeigen. Abbildung 16.28 zeigt einen Benutzer namens `scott` (kaum erkennbar auf der rechten Seite beim Eintrag ProfileImagePath). Doppelklicken Sie im Bereich auf der rechten Seite auf den Eintrag State und setzen Sie den Wert auf 0 (Abbildung 16.29).

Jetzt kommt der letzte Schritt. Wenn es auf der rechten Seite einen Eintrag RefCount gibt, dann setzen Sie ihn auf 0. Wenn es diesen Eintrag nicht gibt, müssen Sie ihn erstellen: Bearbeiten|Neu|DWORD-Wert (32-Bit). Schließen Sie den Registrierungs-Editor und starten Sie den Computer neu. Das Benutzerprofil sollte jetzt wieder funktionieren.

Falls das Profil nicht funktioniert, besteht die nächste Möglichkeit darin, ein neues Benutzerkonto anzulegen und das ältere Benutzerprofil im Wesentlichen zu duplizieren. Starten Sie im abgesicherten Modus und öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Sie benötigen ein Benutzerkonto mit Administratorrechten, um einen neuen Benutzer anzulegen, und genau das werden Sie jetzt tun. Um das supergeheime und versteckte lokale Administratorkonto zu aktivieren, geben Sie folgenden Befehl ein:

```
net user administrator /active:yes
```

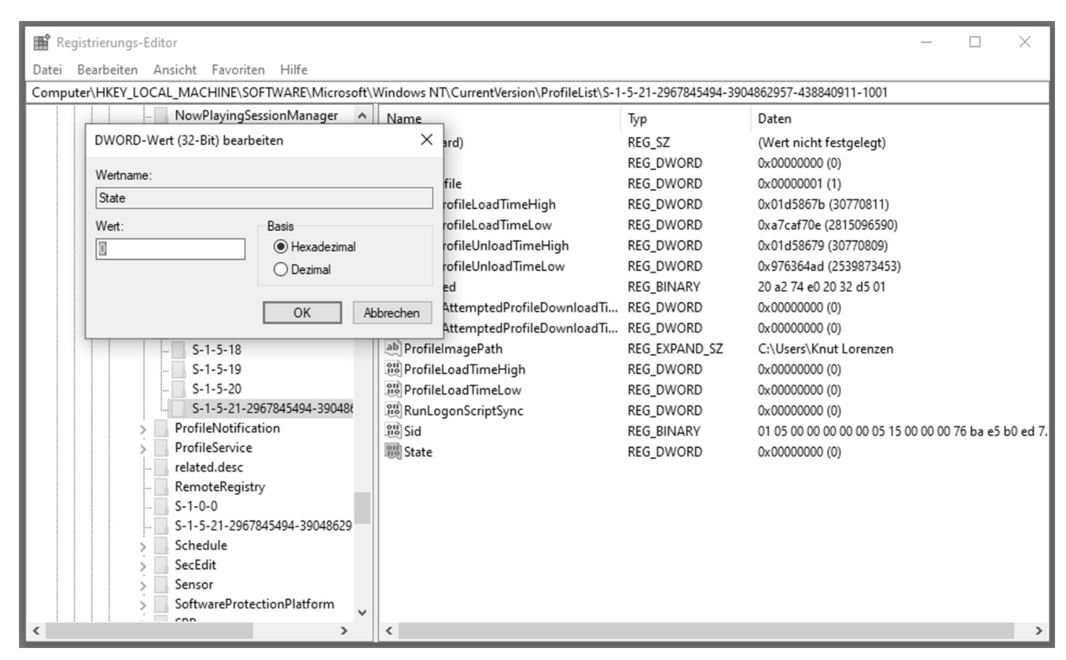


Abb. 16.29: Der Wert von State wird auf 0 gesetzt.

Starten Sie den Computer neu und melden Sie sich mit dem lokalen Administratorkonto an, das Sie soeben aktiviert haben. Legen Sie einen neuen Benutzer an: Einstellungen|Konten|Familie und andere Benutzer|Diesem PC eine andere Person hinzufügen (Abbildung 16.30). Geben Sie dem Benutzerkonto einen eindeutigen Namen. Begeben Sie sich zum Benutzerordner des beschädigten Kontos und kopieren Sie alle Inhalte in den Benutzerordner des neuen Kontos, aber jeweils nur einen Ordner, um zu vermeiden, dass irgendeine der beschädigten Dateien kopiert wird.

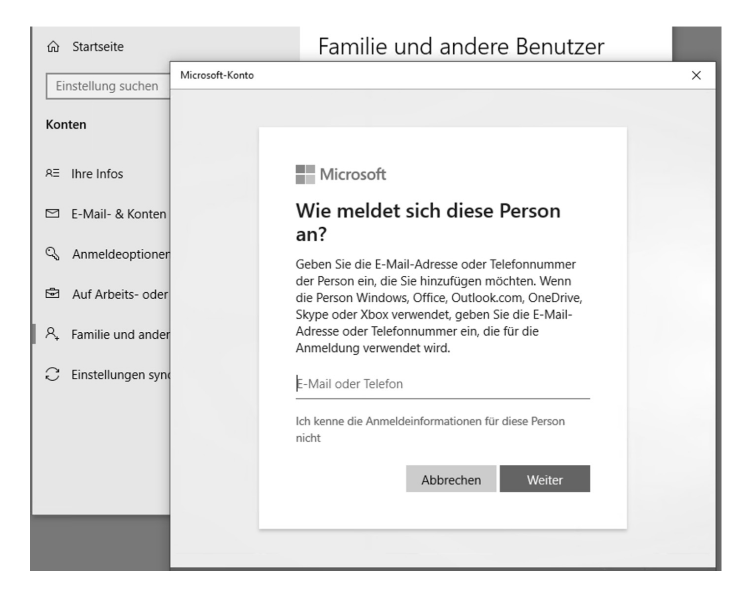


Abb. 16.30: Anlegen eines neuen Benutzerkontos in Windows 10

Nach einem Neustart des Computers sollten Sie sich mit dem neuen Benutzerkonto anmelden und auf alle Dateien des alten Kontos zugreifen können. Wenn Sie das *überprüft* haben, können Sie sich wieder als Administrator anmelden, das beschädigte Benutzerkonto löschen und dem neuen Konto den alten Namen zuweisen.

Die beiden Verfahren zur Wiederherstellung eines beschädigten Benutzerkontos sind umständlich, aber sie funktionieren. Rechnen Sie damit, dass in der Zertifizierungsprüfung Fragen zu diesem Thema vorkommen.

16.2.5 Werkzeuge zur Fehlersuche in der grafischen Benutzeroberfläche

Wenn Sie Windows im abgesicherten Modus oder unter Verwendung einer der anderen Optionen starten können, stehen Ihnen alle Windows-Werkzeuge zur Verfügung. Hat beispielsweise ein fehlerhafter Gerätetreiber die Startprobleme verursacht, können Sie den Geräte-Manager öffnen und dort mit der Fehlersuche beginnen, wie Sie es in früheren Kapiteln gelernt haben. Wenn Sie glauben, ein Dienst oder die Registry hätten das Problem verursacht, informieren Sie sich über die Ereignisanzeige, welche Ereignisse kürzlich stattgefunden haben.

Die Ereignisanzeige

Wenn Sie zur grafischen Benutzeroberfläche gelangen, ist die *Ereignisanzeige* eine der ersten Anlaufstellen, um festzustellen, wodurch die Probleme auf Ihrem Computer verursacht werden. Die Ereignisanzeige ist sozusagen die Quasselstrippe in Windows, die eine Vielzahl von interessanten Vorkommnissen auf Ihrem Computer verrät. Mit ein wenig Aufwand können Sie die Ereignisanzeige für die Aufzeichnung von so ziemlich allem konfigurieren, was Sie jemals über Ihr System wissen wollen.

Wichtig

UNIX-Systeme wie macOS und verschiedene Linux-Distros verwenden ein Werkzeug namens `syslog`, um Informationen zu erzeugen, die in Protokolldateien abgelegt werden. Anwendungsprogramme verwenden `syslog`, um die Anwendung betreffende Vorkommnisse zu protokollieren. Das funktioniert auch über das Netzwerk, und Sie können sich sicherlich vorstellen, wie nützlich das ist! `syslog` ist jedoch kein Programm, wie die Ereignisanzeige. Programme verwenden `syslog`, um Ereignisse aufzuzeichnen. In den meisten Linux-Distros finden Sie die Protokolldateien im Verzeichnis `/var/log`. `syslog` wird von Drittherstellern auch unter Windows unterstützt, es ist also nicht auf UNIX-basierte Systeme beschränkt.

Beachten Sie auch, dass die Ereignisanzeige nicht nur zur Fehlersuche in Windows dient, sondern auch ein leistungsfähiges Sicherheitswerkzeug ist (wie Sie in Kapitel 27 noch erfahren werden). Aber lassen Sie uns zunächst die Ereignisanzeige näher betrachten.

Nach dem Öffnen der Ereignisanzeige (über SYSTEMSTEUERUNG |VERWALTUNG|EREIGNISANZEIGE) wird Ihnen die Standardbenutzeroberfläche präsentiert (Abbildung 16.31).

Beachten Sie die vier Leisten in der Mitte: ÜBERSICHT, ZUSAMMENFASSUNG DER ADMINISTRATIVEN EREIGNISSE, ZULETZT ANGEZEIGTE KNOTEN und PROTOKOLLZUSAMMENFASSUNG. Schenken Sie insbesondere der ZUSAMMENFASSUNG DER ADMINISTRATIVEN EREIGNISSE Beachtung. Hier sind die Ereignisse nach verschiedenen Ebenen sortiert: KRITISCH, FEHLER, WARNUNG, INFORMATIONEN, ÜBERWACHUNG ERFOLGREICH und ÜBERWACHUNG GESCHEITERT. Abbildung 16.32 zeigt eine typische Zusammenfassung mit einer ausgewählten Warnung. Klicken Sie auf ein Ereignis, um eine *Ansicht* mit einer genaueren Beschreibung anzuzeigen. (Ich habe den Aktionsbereich ausgeblendet, damit mehr vom mittleren Bereich zu sehen ist.)

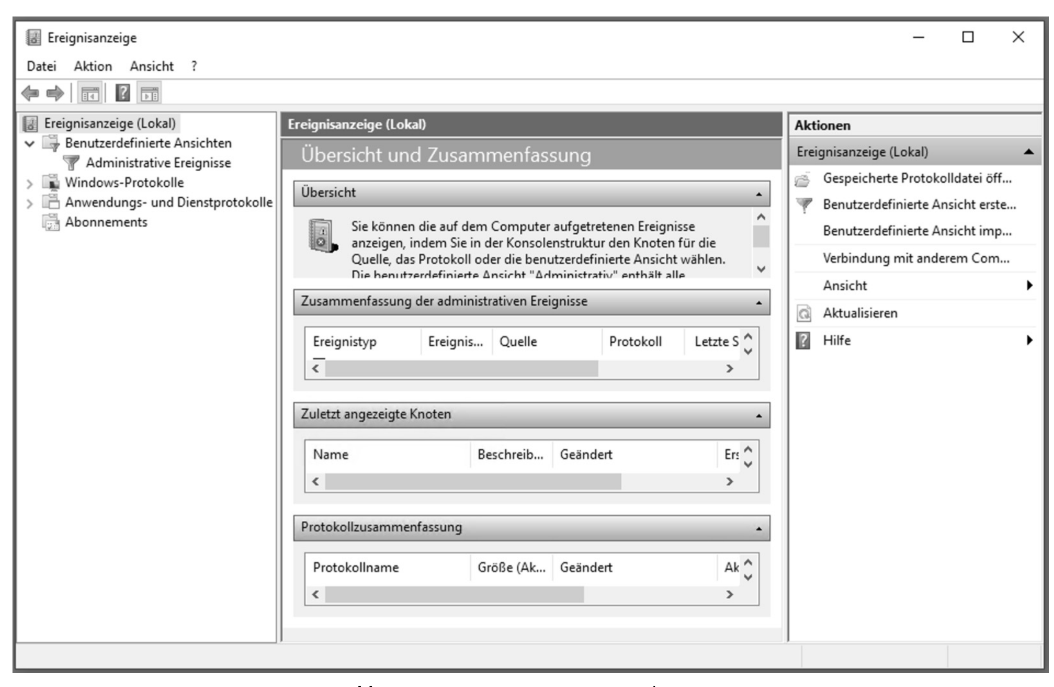


Abb. 16.31: Ereignisanzeige in Windows 10

Ereignisanzeige

Datei Aktion Ansicht ?

Ereignisanzeige (Lokal)
Benutzerdefinierte Ansichten
Administrative Ereignisse
Windows-Protokolle
Anwendungs- und Dienstprotokolle
Abonnements

Ereignisanzeige (Lokal)

Übersicht und Zusammenfassung — Zuletzt aktualisiert: 19.10.2019 16:00:29

Übersicht

Sie können die auf dem Computer aufgetretenen Ereignisse anzeigen, indem Sie in der Konsolenstruktur den Knoten für die Quelle, das Protokoll oder die benutzerdefinierte Ansicht wählen. Die benutzerdefinierte Ansicht "Administrativ" enthält alle administrativen Ereignisse, unabhängig von der Quelle. Eine Zusammenfassung aller Protokolle wird unten angezeigt.

Zusammenfassung der administrativen Ereignisse

Ereignistyp	Ereignis...	Quelle	Protokoll	Letzte Stu...	24 Stunden	7 Tage
Warnung	-	-	-	0	34	192
	4	Kernel-EventTr...	Microsoft...	0	0	7
	36	TerminalServic...	Microsoft...	0	2	8

Zuletzt angezeigte Knoten

Name	Beschreib...	Geändert	Erstellt
Benutzerdefinierte Ansic...	Kritische, ...	Nicht zutreffend	Nicht zutreffend
Windows-Protokolle\Sys...	Nicht zutr...	19.10.2019 15:45:15	05.07.2019 19:08:20
Windows-Protokolle\Inst...	Nicht zutr...	19.10.2019 15:10:43	05.07.2019 19:08:23

Protokollzusammenfassung

Protokollname	Größe (Ak...	Geändert	Aktiviert	Beibehaltungsrichtlinie
Windows PowerShell	68 KB/15 ...	14.10.2019 19:03:31	Aktiviert	Ereignisse bei Bedarf üb...
System	2,07 MB/2...	19.10.2019 15:45:15	Aktiviert	Ereignisse bei Bedarf üb...
Sicherheit	20,00 MB/...	19.10.2019 15:59:36	Aktiviert	Ereignisse bei Bedarf üb...

Abb. 16.32: Warnung in der Ereignisanzeige

Die Ereignisanzeige enthält weiterhin die klassischen Protokolle (Anwendung, Sicherheit, System), tendiert aber bei der Anzeige der Protokollinhalte deutlich zu den neuen Ansichten. Sie können damit Protokolle nach Start-/Endzeit, Fehlerebene usw. filtern, sodass sie hervorragend für Berichte geeignet sind. Verwenden Sie dazu die voreingestellten Ansichten oder erstellen Sie Ihre eigenen (Abbildung 16.33).

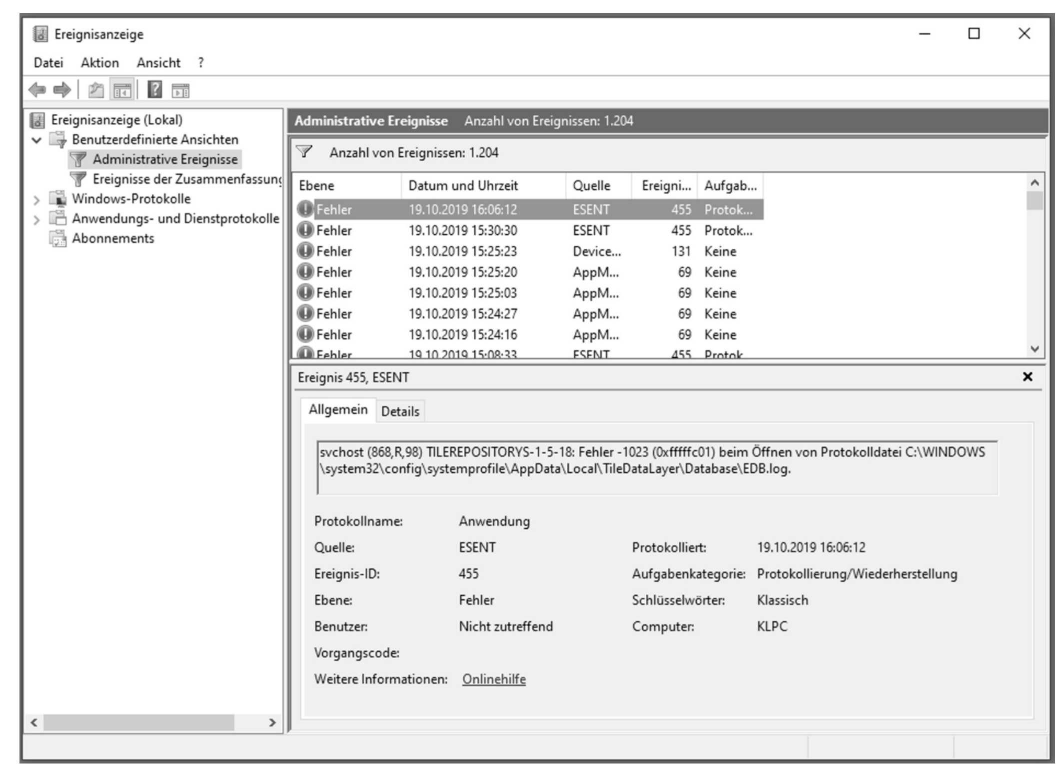


Abb. 16.33: Benutzerdefinierte Ansicht

Hinweis

Standardmäßig speichert die Ereignisanzeige Protokolldateien mit der Endung `.evtx` im Verzeichnis `C:\Windows\System32\Winevt\Logs`.

Alle Ereignisse werden in Protokolldateien gespeichert, die gewissen Einschränkungen unterliegen. Für sie gibt es eine maximale Größe, einen Speicherort und ein bestimmtes Verhalten beim Überschreiten dieser Größe (wie etwa Überschreiben alter Einträge oder eine Fehlermeldung). Abbildung 16.34 zeigt ein typisches EIGENSCHAFTEN-Dialogfeld eines Protokolls in Windows 10. Beachten Sie hier, dass Änderungen an den Protokolldateien der Ereignisanzeige Administratorrechte erfordern.

Wichtig

Wenn Sie vor einer Situation stehen, in der ein Gerät ausgefallen ist und dies zu Startproblemen von Windows führt, sollten Sie das bevorzugte Werkzeug bei Hardwareproblemen einsetzen: den Geräte-Manager. Lesen Sie gegebenenfalls in den Kapiteln über Hardware nach.

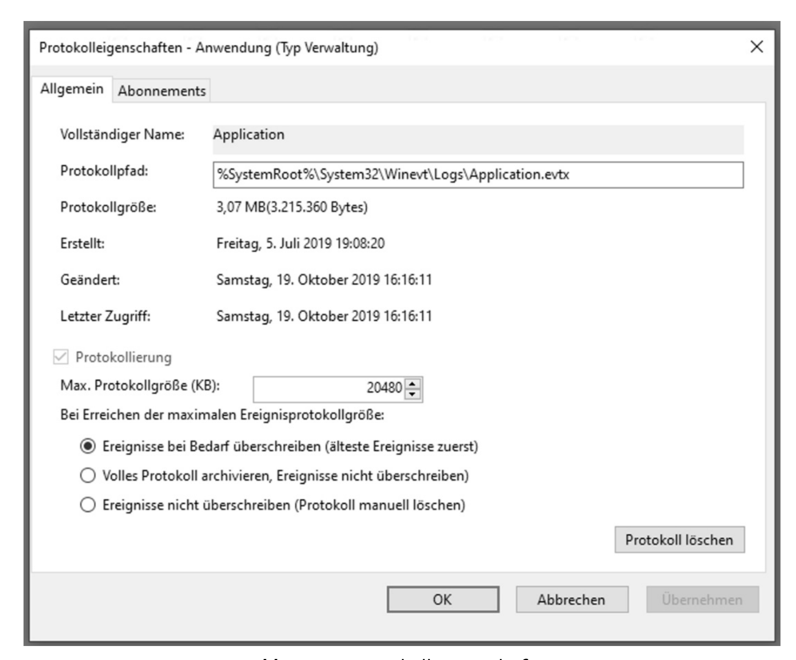


Abb. 16.34: Protokolleigenschaften

Automatisch gestartete Programme

Windows unterstützt das automatische Laden von Programmen beim Start. Meist ist das auch wirklich praktisch, weshalb wohl alle Windows-PCs diese Möglichkeit nutzen. Autostart-Programme werden dann problematisch, wenn sich eines davon fehlerhaft verhält und Sie dessen Ausführung unterbinden müssen! Benutzen Sie das Systemkonfigurationsprogramm (Windows 7) oder den Task-Manager (Windows 8/8.1/10), um den automatischen Start solcher Programme vorübergehend zu deaktivieren. Wenn Sie den automatischen Start dauerhaft abschalten möchten, suchen Sie in dem jeweiligen Programm nach einer Option, um dies zu erledigen (Abbildung 16.35).



Abb. 16.35: Deaktivieren des automatischen Programmstarts

Wichtig

Dienste und Programme, die zu Windows gehören, können Sie in der Systemsteuerung im Bereich PROGRAMME UND FEATURES deaktivieren. Auf der linken Seite gibt es die Option WINDOWS-FEATURES AKTIVIEREN ODER DEAKTIVIEREN. An gleicher Stelle können Sie einen Dienst oder eine Anwendung später wieder aktivieren.

Dienste

Windows lädt beim Starten verschiedene Dienste. Wenn einer der kritischen Dienste nicht geladen werden kann, teilt Ihnen Windows dies sofort in einer Fehlermeldung mit. Das entscheidende Wort ist hier »kritisch«. Windows meldet nicht *alle* Fehler, die beim Starten von Diensten auftreten. Wenn ein in den Augen von Windows weniger kritischer Dienst nicht gestartet werden kann, wartet es normalerweise, bis Sie ein Programm zu verwenden versuchen, das diesen Dienst benötigt, bevor es Ihnen eine Fehlermeldung präsentiert (Abbildung 16.36).

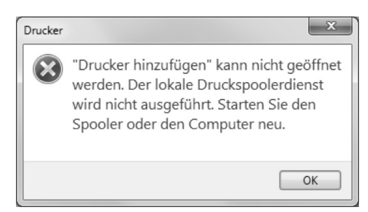


Abb. 16.36: Fehlermeldung zu einem nicht laufenden Dienst

Sie finden die Systemdienste unter SYSTEMSTEUERUNG|VERWALTUNG|DIENSTE. Dort können Sie überprüfen, ob der von Ihnen benötigte Dienst ausgeführt wird. Ist dies nicht der Fall, starten Sie ihn. Beachten Sie außerdem, dass jeder Dienst einen Starttyp hat – AUTOMATISCH, MANUELL oder DEAKTIVIERT. Der Starttyp legt fest, wann der Dienst gestartet wird. Häufig sind Dienste auf MANUELL gesetzt, obwohl sie eigentlich den Starttyp AUTOMATISCH haben sollten, damit sie beim Booten von Windows gestartet werden (Abbildung 16.37).

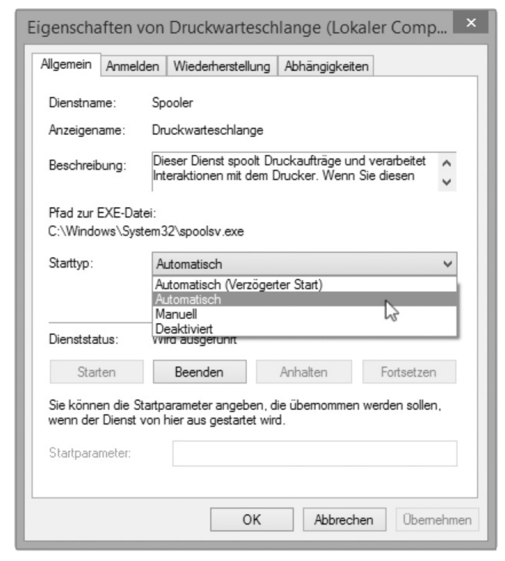


Abb. 16.37: Einen Dienst automatisch starten

Task-Manager und Eingabeaufforderung

Aus Kapitel 12 wissen Sie, dass Sie mit dem Task-Manager irrlichternde Prozesse beenden können, die sich auf normale Weise nicht schließen lassen. So können Sie beispielsweise schnell ein Programm beenden, das die CPU auslastet, indem Sie es auf der Registerkarte PROZESSE mit der rechten Maustaste anklicken und TASK BEENDEN auswählen. Sie können sämtliche Anwendungen und Programme anzeigen oder beenden, wenn diese nicht mehr funktionieren. Mit der Tastenkombination `Strg` + `Alt` + `ESC` können Sie ihn direkt öffnen, und durch Drücken von `Strg` + `Alt` + `Entf` gelangen Sie zu einer Liste, aus der Sie ihn auswählen können.

Wenn Sie lieber mit der Kommandozeile arbeiten, geben Sie auf der Eingabeaufforderung `tasklist` ein, um eine Liste mit den Namen und IDs aller laufenden Prozesse anzuzeigen. Mittels `taskkill` und Angabe von Name oder ID können Sie einen Prozess beenden. In Kapitel 12 können Sie die Details zur Verwaltung von Prozessen auf der Kommandozeile nachlesen. Falls Sie die PowerShell verwenden, lauten die Befehle `tasklist` und `kill`.

Systemdateien

Windows stützt sich auf DLL-Dateien (Dynamic Link Library). Fast alle von Windows verwendeten Programme und mit Sicherheit alle wichtigen Programme rufen DLL-Dateien auf, um Windows zu seiner Schwerstarbeit zu veranlassen.

Windows schützt alle kritischen DLL-Dateien sehr sorgfältig, aber manchmal erhält man dennoch eine Fehlermeldung, die besagt, dass Windows eine bestimmte DLL nicht laden kann. Das passiert zwar selten, aber die Dateien des Kernsystems von Windows können so beschädigt werden, dass Windows nicht mehr korrekt startet. Normalerweise sieht man dann die Meldung »Fehler beim Laden von `XXXX.DLL`« oder etwas Ähnliches. Manchmal werden aber auch einfach Programme nicht mehr gestartet, wenn Sie deren Symbole doppelt anklicken. In diesen Fällen können Sie die *Dateisystemprüfung* (*SFC – System File Checker*), die Sie aus Kapitel 15 kennen, über die Eingabeaufforderung ausführen. Sie überprüft verschiedene kritische Dateien, einschließlich des so wichtigen DLL-Caches.

Wichtig

In macOS und Linux können Sie im Terminal den Befehl `kill` verwenden, um laufende Programme zu beenden, ähnlich wie in der Eingabeaufforderung oder der PowerShell. Rechnen Sie damit, dass diese Befehle in der Zertifizierungsprüfung vorkommen.

Systemwiederherstellung

Die Systemwiederherstellung ist der letzte Ausweg bei der Behebung größerer Windows-Probleme. Gehen Sie dazu wie in diesem Kapitel bereits beschrieben vor. Beachten Sie jedoch, dass Sie auch einen Wiederherstellungspunkt laden können. Folgen Sie dazu den in Kapitel 14 erläuterten Schritten. Die Systemwiederherstellung kann sich auch als hilfreich erweisen, wenn ein Computer sehr langsam ist. Manche Systeme werden im Laufe der Zeit immer langsamer, weil schlecht programmierte Anwendungen sie belasten. Die Wiederherstellung des Zustands zu einem früheren Zeitpunkt kann einem kränkelnden PC wieder Schwung verleihen, ohne dass es den Benutzer oder den Techniker allzu große Anstrengungen kostet.

Wichtig

Wenn Windows startet, aber das Betriebssystem nicht richtig funktioniert oder sehr langsam arbeitet, gibt es eine weitere Möglichkeit, das Problem zu beheben. Die Option INSTALLATION REPARIEREN wird von Windows aus gestartet. Sie führen die Datei `setup.exe` der Betriebssystemmedien (DVD oder USB-Speicherstick) aus und installieren Windows im Wesentlichen neu. Sie haben dabei die Möglichkeit, Ihre persönlichen Dateien und Programme zu behalten. Wenn Sie sich entscheiden, alles zu behalten, wird die

Windows-Installationsroutine nur Systemdateien und Gerätetreiber überschreiben und im Internet nach Aktualisierungen suchen (sofern der Computer über eine Internetverbindung verfügt).

Deaktivieren Sie in den UEFI-Einstellungen den sicheren Start und auch alle Anti-Malware-Programme von Drittherstellern, bevor Sie anfangen. Es ist auch immer eine gute Idee, vor derartigen Aktionen eine Sicherheitskopie der eigenen Daten anzufertigen. Wenn aus irgendwelchen Gründen etwas schiefgeht, sind zumindest Ihre Daten in Sicherheit.

16.2.6 Werkzeuge zur Fehlersuche in Windows

Die Systemsteuerung bietet eine Reihe weiterer Werkzeuge, die Techniker benötigen, um eine Vielzahl von Problemen zu beheben. Hier sind insbesondere die PROBLEMBEHANDLUNG und SICHERHEIT UND WARTUNG/WARTUNGSCENTER zu nennen.

Das Applet PROBLEMBEHANDLUNG bietet eine Auswahl gängiger Lösungen für Probleme an, die sowohl die Hardware als auch Anwendungen betreffen (Abbildung 16.38). Das Startfenster bietet vier verschiedene Kategorien: PROGRAMME, HARDWARE UND SOUND, NETZWERK UND INTERNET sowie SYSTEM UND SICHERHEIT. (In Windows 7 gibt es eine fünfte Kategorie, DARSTELLUNG UND ANPASSUNG, um Probleme mit der Anzeige zu beheben.) Erkunden Sie das Werkzeug am besten selbst – ich werde an den entsprechenden Stellen im Buch darauf zurückkommen. Aber hier zeige ich ein paar Highlights.

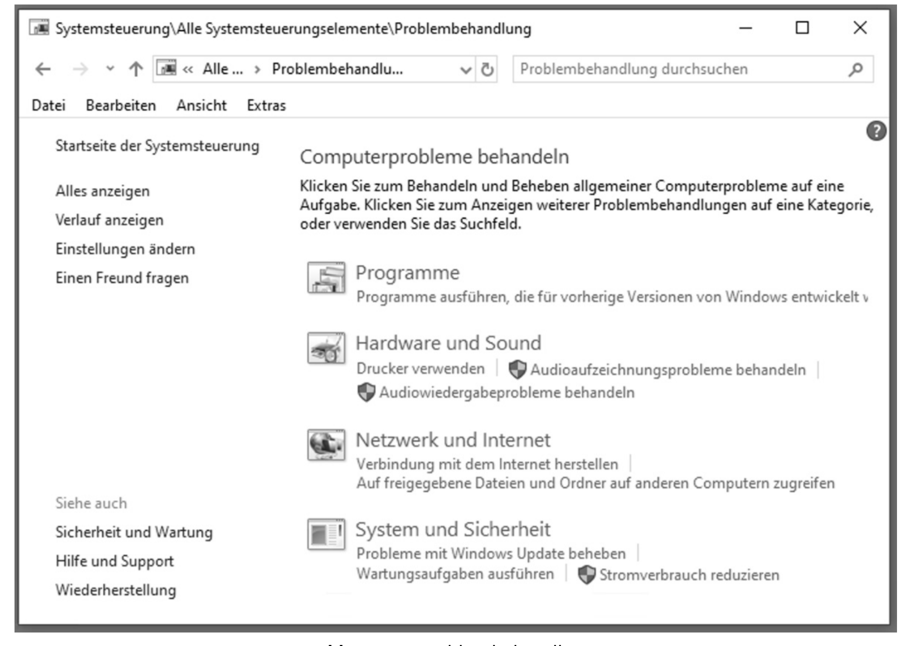


Abb. 16.38: Problembehandlung

Klicken Sie in der Kategorie HARDWARE UND SOUND auf DRUCKER VERWENDEN, wenn Sie Probleme mit dem Drucken haben. Daraufhin öffnet sich ein Assistent, der Sie bei der Fehlerbehebung unterstützt (Abbildung 16.39). Klicken Sie auf WEITER und folgen Sie den Anweisungen. Der Assistent testet die Druckerwarteschlange, prüft die Treiber und so weiter. In Kapitel 26 werden wir Drucker und die Fehlerbehebung bei Druckern eingehend betrachten, aber das Applet PROBLEMBEHANDLUNG ist ein guter Ausgangspunkt.

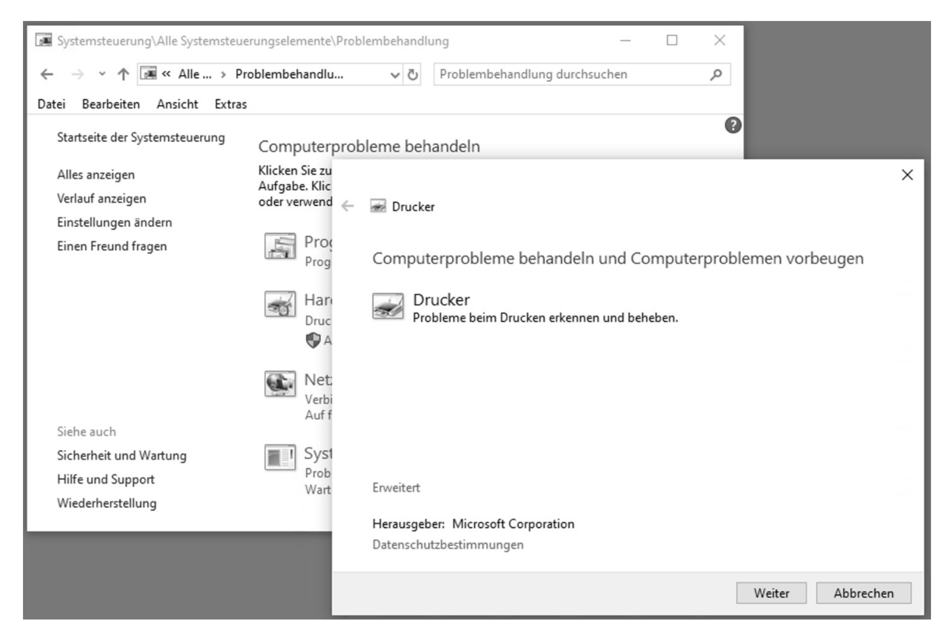


Abb. 16.39: Der Assistent zur Fehlerbehebung beim Drucken im Applet PROBLEMBEHANDLUNG

Verwenden Sie die Optionen der Kategorie NETZWERK UND INTERNET, um die Netzwerkeinstellungen zu aktualisieren. Wir werden uns in Kapitel 19 ausführlich damit befassen, aber hier können Sie jedenfalls nach Fehlern suchen, wenn die Netzwerkverbindung nicht richtig funktioniert oder es Probleme mit dem Zugriff auf Ressourcen über das Netzwerk gibt.

Wenn Ihnen Windows Update Schwierigkeiten bereiten, beispielsweise weil ein Gerät nach dem Einspielen eines Patches nicht mehr funktioniert, sollten Sie in der Kategorie SYSTEM UND SICHERHEIT auf PROBLEME MIT WINDOWS UPDATE BEHEBEN klicken. Dann wird ein Assistent zur Behebung von Fehlern gestartet, die im Zusammenhang mit Windows Update auftreten können (Abbildung 16.40). Folgen Sie auch hier den Anweisungen auf dem Bildschirm. Klicken Sie auf DIESE KORREKTUR ANWENDEN oder auf DIESE KORREKTUR ÜBERSPRINGEN, sobald der Assistent die Überprüfung anstehender Updates abgeschlossen hat.

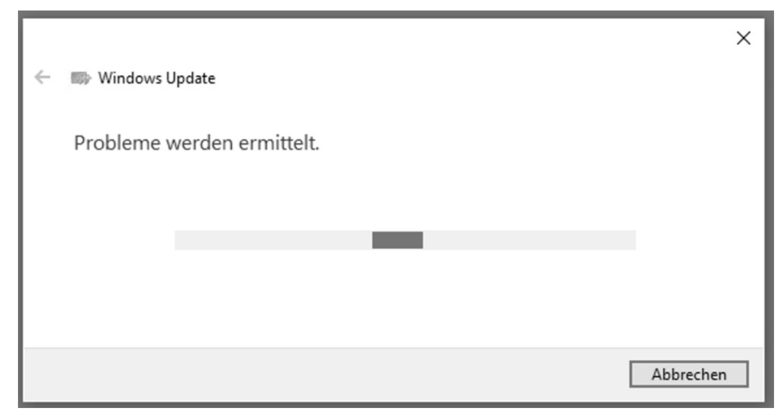


Abb. 16.40: Der Assistent zur Fehlerbehebung mit Windows Update bei der Arbeit

Sicherheit und Wartung/Wartungscenter

SICHERHEIT UND WARTUNG in Windows 10 und das WARTUNGSCENTER in Windows 7/8/8.1, in denen sich eine Sammlung von Benachrichtigungen, Warnungen und Wartungsmeldungen findet, könnten für viele Techniker vielleicht schon bald die EREIGNISANZEIGE als erste Anlaufstelle bei Problemen ersetzen. Die Werkzeuge erlauben einen schnellen Überblick über das System (Abbildung 16.41).

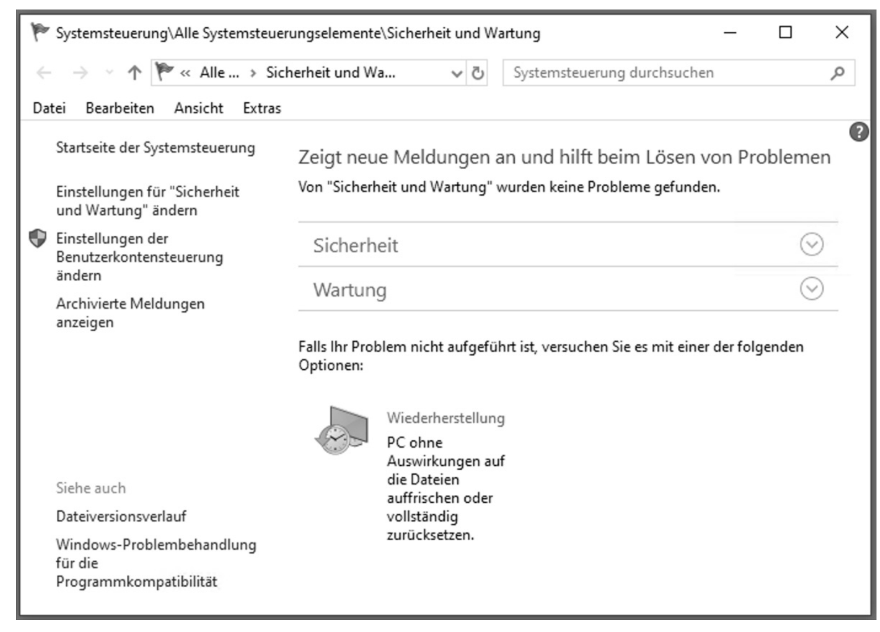


Abb. 16.41: Sicherheit und Wartung

SICHERHEIT UND WARTUNG/WARTUNGSCENTER sammeln die Informationen nur und bedienen sich dabei wohlbekannter Werkzeuge (wie Ereignisanzeige, Windows Update, Windows Firewall und Benutzerkontensteuerung) und stellen diese in leicht lesbarer Form bereit. Auf Wunsch können Sie SICHERHEIT UND WARTUNG/WARTUNGSCENTER mitteilen, wo sie nach Informationen suchen sollen. Klicken Sie dazu auf EINSTELLUNGEN FÜR "SICHERHEIT UND WARTUNG" ÄNDERN oder auf WARTUNGSCENTEREINSTELLUNGEN ÄNDERN (Abbildung 16.42).

Für den Fall, dass Sie auf Probleme stoßen, enthalten SICHERHEIT UND WARTUNG/WARTUNGSCENTER eine ganze Reihe von Verknüpfungen, mit denen Sie schnell zum gerade erforderlichen Werkzeug gelangen. Es gibt Verknüpfungen zu:

- Einstellungen der Benutzerkontensteuerung
- Sichern und Wiederherstellen
- Windows Update
- Problembehandlungs-Assistent
- Systemwiederherstellung
- Wiederherstellung

Auch wenn SICHERHEIT UND WARTUNG bzw. WARTUNGSCENTER eigentlich nur die Informationen anderer Dienstprogramme wiedergibt, vereinfacht und beschleunigt es die Fehlersuche doch erheblich. Zusammen mit den Verknüpfungen zu den meisten Dienstprogrammen stellen SICHERHEIT UND WARTUNG/WARTUNGSCENTER einen guten Ausgangspunkt für die Behebung von Problemen dar, wenn auf einem PC mit Windows etwas schiefgeht.

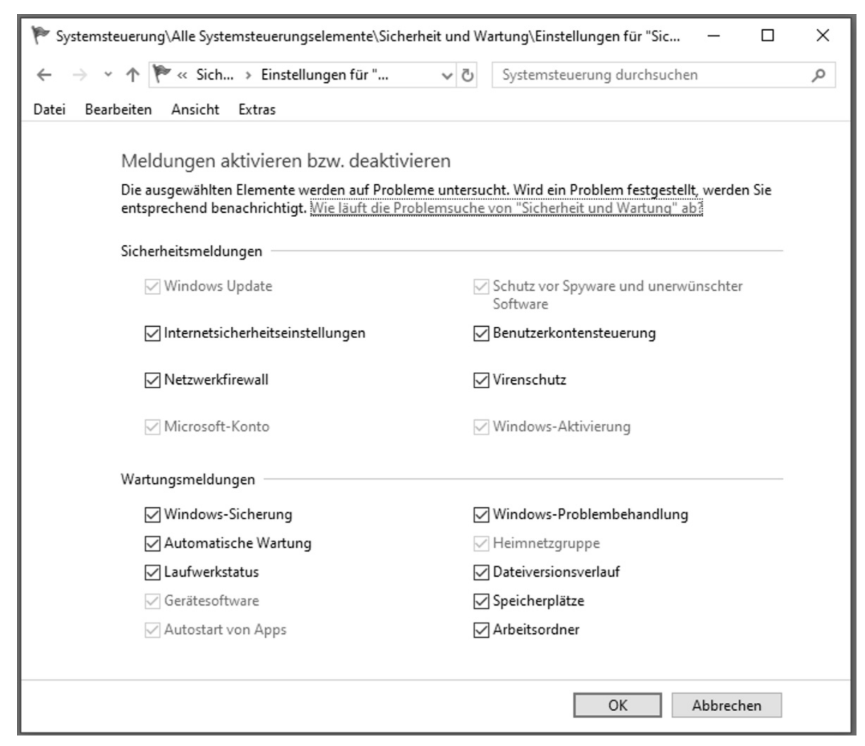


Abb. 16.42: Einstellungen für SICHERHEIT UND WARTUNG ändern

Tipp: Sicherheit und Wartung

Falls Sie noch keine Gelegenheit hatten, SICHERHEIT UND WARTUNG in Windows 10 zu erkunden, ist jetzt der richtige Zeitpunkt gekommen! Öffnen Sie das Werkzeug in der Systemsteuerung oder direkt, indem Sie im Suchfeld `Sicherheit und ...` eingeben und den Treffer in der Liste auswählen. Sind Netzwerkfirewall und Virenschutz aktiviert? Gibt es irgendwelche Meldungen, um die Sie sich kümmern müssen? Welche Verhaltensweisen können Sie ändern, wenn Sie auf EINSTELLUNGEN FÜR "SICHERHEIT UND WARTUNG" ÄNDERN klicken? Und wenn Sie schon dabei sind, klicken Sie auch unten links auf ARCHIVIERTE MELDUNGEN ANZEIGEN, um das Tool zu erkunden.

16.3 Anwendungsprobleme

Programmierer wollen Anwendungen entwickeln, die gut funktionieren, ein bestimmtes Problem für sie lösen und gut genug sind, um damit Geld zu verdienen. Nun sind PCs aber kompliziert und es ist für die Programmierer nicht ganz einfach, immer alle möglichen Kombinationen von Hard- und Software zu berücksichtigen.

Anwendungsprobleme zeigen sich auf verschiedene Weise. Meistens gibt es Probleme beim Installieren oder beim Deinstallieren. Verschiedene Betriebssystemversionen können darüber hinaus Kompatibilitätsprobleme bereiten. Eine andere typische Schwierigkeit sind Dateien, auf die ein Programm zugreifen muss, diese aber nicht vorhanden sind oder sich nicht öffnen lassen. Schlampig oder schlecht programmierter Code, der zu Abstürzen des Programms oder des Betriebssystems führt, ist nur in den wenigsten Fällen ausschlaggebend, wenn es zu Problemen mit Anwendungen kommt. Zu guter Letzt können beschädigte Programme auch beschädigte Dateien nach sich ziehen, aber Windows besitzt Werkzeuge zum Wiederherstellen vorheriger Versionen von Dateien und Ordnern.

Wichtig

Gelegentlich trifft man auf Anwendungen, die mit einer Fehlermeldung reagieren, wenn die Uhrzeiteinstellungen in Windows und im BIOS voneinander abweichen. Es ist möglich, dass die Anwendung deswegen nicht startet. Auch wenn die CMOS-Batterie sehr schwach oder leer ist und der Computer längere Zeit nicht online ist, kann es zu Abweichungen zwischen BIOS- und Systemzeit kommen. Wenn der Computer wieder Verbindung zu einem Zeitserver aufnehmen kann, gibt es eine kurze Fehlermeldung (zumindest in den Protokolldateien). Hierbei handelt es sich sowohl um ein Hardware- (die Batterie) als auch um ein Softwareproblem. Wird die Windows-Systemzeit zurückgesetzt, gilt dies auch für die BIOS-Zeit.

16.3.1 Installationsprobleme

Nahezu allen Windows-Programmen liegt irgendein praktisches Installationsprogramm bei. Wenn Sie die Disc ins Laufwerk legen oder den USB-Stick einstöpseln, sucht Windows nach einer Datei namens `autorun.inf`, in der vermerkt ist, welches Programm ausgeführt werden soll, für gewöhnlich heißt es `setup.exe`. Wenn Sie die Anwendung aus dem Internet heruntergeladen haben, doppelklicken Sie auf das Installationsprogramm, um die Installation durchzuführen. Bei beiden Methoden können Sie anschließend das eigentliche Programm starten. Es könnte kaum einfacher sein.

Wichtig

Dadurch, dass Windows standardmäßig automatisch nach der Datei `autorun.inf` sucht, entsteht eine Sicherheitslücke. Jemand packt eine Schadsoftware auf eine Disc oder einen USB-Stick und schreibt eine `autorun.inf`-Datei, die darauf verweist. Sie legen die Disc ein oder schließen den Speicherstick an – und schon ist das Kind in den Brunnen gefallen! Wenn jemand physischen Zugriff auf Ihren Computer hat und sich mit Administratorrechten anmelden kann, haben Sie natürlich ohnehin schon die Kontrolle über Ihren Rechner verloren, und die Sicherheitslücke beim Einlegen oder Anschließen von Medien spielt dann kaum noch eine Rolle. Dessen ungeachtet sollten Sie wissen, dass mit dem Registrierungs-Editor bis zu sechs verschiedene Einstellungen geändert werden müssen, um Windows dieses Verhalten abzugewöhnen.

Programme, die etwas auf sich halten, sollten sich auch ebenso einfach wieder deinstallieren lassen. Meist finden Sie eine Option zur Deinstallation im Ordner des Programms im Start-Menü. Und immer (außer bei Programmen mit einem mangelhaft konfigurierten Installationsprogramm) sollte die Anwendung entweder im Applet PROGRAMME UND FEATURES in der Systemsteuerung oder unter APPS & FEATURES in den Einstellungen angezeigt werden (Abbildung 16.43).

Hinweis

Denken Sie daran, dass Sie unter allen Windows-Versionen lokale Administratorrechte zum Installieren von Anwendungen benötigen.

Bei Programmen, die sich nicht installieren lassen, ist der Fehler üblicherweise nicht bei ihnen selbst zu suchen. Meist verhindern irgendwelche Windows-Probleme, dass die Installation klappt, insbesondere fehlende andere Programme, die eine Anwendung benötigt, um funktionieren zu können. Eines der besten Beispiele ist das verbreitete *.NET-Framework* von Microsoft. Bei .NET handelt es sich um eine Erweiterung des Windows-Betriebssystems, die für die Unterstützung einer Reihe von Funktionen sorgt, zu denen mächtigere Tools für die Benutzerschnittstelle und den viel flexibleren Datenbankzugriff zählen. Wenn ein Programm so geschrieben wurde, dass es das .NET-Framework benutzt, dann muss .NET selbst auch installiert sein. Wenn das nicht der Fall ist, dann sollte die Anwendung zwar in den meisten Fällen versuchen, es bei der eigenen Installation gleich mitzuinstallieren, aber darauf können Sie sich nicht verlassen. Falls .NET fehlt oder die installierte Version zu alt ist (es hat seit der ersten Veröffentlichung von .NET im Jahr 2002 etliche Versionen gegeben), werden einige der unverständlichsten Fehlermeldungen in der Geschichte der Windows-Anwendungen angezeigt.



Abb. 16.43: APPS & FEATURES in den Einstellungen

Abbildung 16.44 zeigt ein derartiges Beispiel unter Windows 7, in dem der vSphere-Client von VMware wegen einer falschen .NET-Version nicht ausgeführt werden kann. Nur schade, dass die Fehlermeldung keine wirklich nützlichen Hinweise gibt!

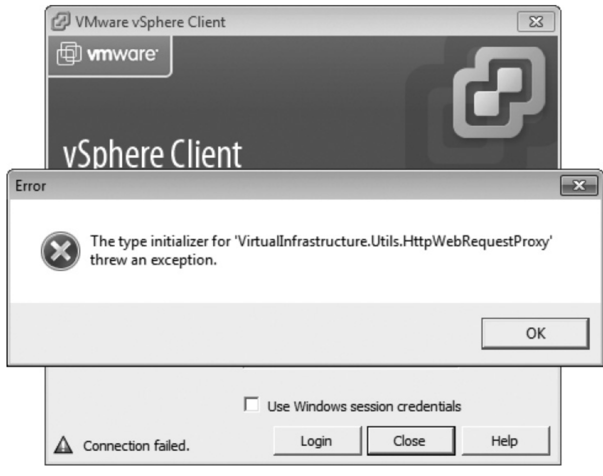


Abb. 16.44: .NET-Fehler

Bei derartigen Fehlern müssen Sie sich unweigerlich im Internet auf die Suche begeben und dabei den Namen der Anwendung und die Fehlermeldung als Suchbegriff eingeben. Wie gravierend der Fehler auch sein mag, normalerweise haben bereits andere Leute darunter zu leiden gehabt. Sie müssen also nur noch herausfinden, wie diese den Fehler umgehen oder beheben konnten.

16.3.2 Probleme beim Deinstallieren

Das größte Problem beim Deinstallieren besteht wohl darin, dass Anwender es ohne Administratorrechte durchzuführen versuchen. Wenn beim Deinstallieren Fehlermeldungen angezeigt werden, melden Sie sich als Administrator an und schon sollte es klappen. Vergessen Sie auch nicht, dass Sie die meisten der im Menü PROGRAMME angezeigten Deinstallationsprogramme mit der rechten Maustaste anklicken und die Option ALS ADMINISTRATOR AUSFÜHREN wählen können, um die Deinstallation mit Administratorrechten durchzuführen (Abbildung 16.45).

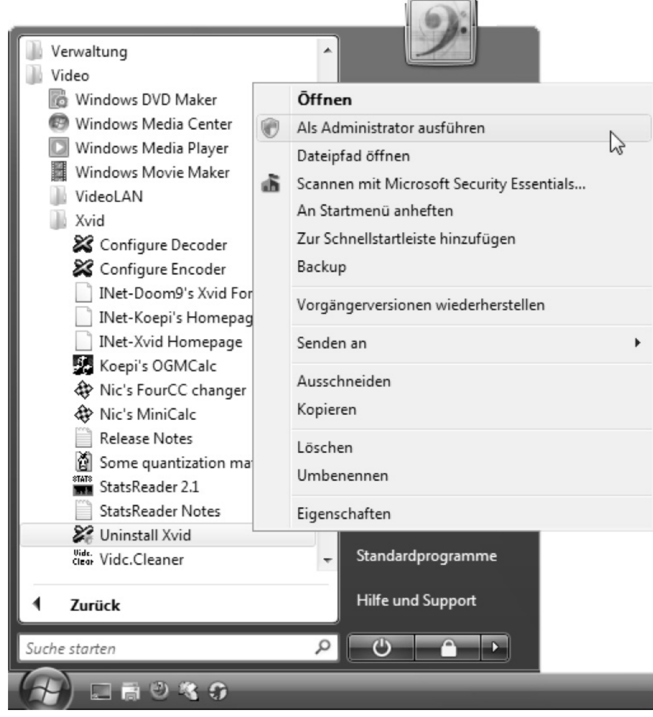
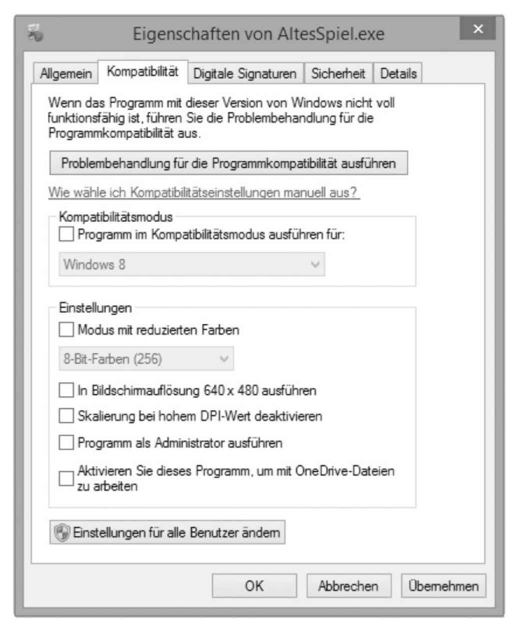


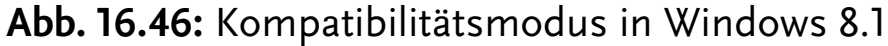
Abb. 16.45: ALS ADMINISTRATOR AUSFÜHREN im Kontextmenü auswählen

16.3.3 Kompatibilität

Die meisten neueren Anwendungen werden auch für die jeweils aktuellen Windows-Versionen geschrieben. Aber es gibt immer wieder neue Windows-Versionen, mit denen ältere Programme Schwierigkeiten haben. Manchmal (wie beim Umstieg von Windows 7 auf Windows 8) sind die Unterschiede in den Versionen derart gering, dass nur wenige oder gar keine Kompatibilitätsprobleme auftreten, wenn eine für eine ältere Windows-Version entwickelte Anwendung ausgeführt wird. In anderen Fällen, wie z.B. bei Anwendungen, die programmiert wurden, als Windows XP aktuell war, hat sich der Unterbau des Betriebssystems zwischenzeitlich so stark geändert, dass Sie bestimmte Maßnahmen ergreifen müssen, damit die älteren Programme weiterhin laufen. Windows bietet zur Unterstützung älterer Anwendungen daher verschiedenartige Kompatibilitätsmodi an.

Zu diesem Zweck gibt es im EIGENSCHAFTEN-Dialogfeld jeder ausführbaren Datei die Registerkarte KOMPATIBILITÄT (Abbildung 16.46). Auf dieser können Sie auswählen, welche Windows-Version emuliert werden soll, und in vielen Fällen ist das auch schon alles, was Sie tun müssen, damit ältere Programme auch weiterhin ausgeführt werden können (Abbildung 16.47).




Abb. 16.46: Kompatibilitätsmodus in Windows 8.1

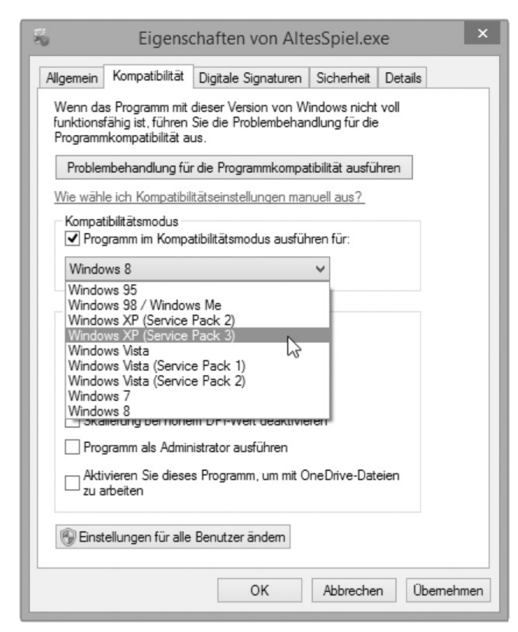


Abb. 16.47: Optionen des Kompatibilitätsmodus in Windows 8.1

Auf der Registerkarte KOMPATIBILITÄT können Sie auch eine Reihe weiterer Einstellungen vornehmen:

- **Modus mit reduzierten Farben**: Viele ältere Windows-Programme sind dafür ausgelegt, mit 256 Farben ausgeführt zu werden. Bei neueren Windows-Versionen, die mehr Farben unterstützen, kann dies zu Problemen führen.
- **In Bildschirmauflösung 640 x 480 ausführen**: Einige (miserabel programmierte) ältere Programme gehen davon aus, dass der Bildschirm eine Auflösung von 640 x 480 besitzt. Diese Einstellung erlaubt deren Ausführung.
- **Desktopgestaltung deaktivieren (Windows 7)**: Durch diese Option werden Darstellungsoptionen wie z.B. Aero abgeschaltet. Solche anspruchsvolleren Darstellungsmethoden verlangsamen ältere Programme oftmals.
- **Skalierung bei hohem DPI-Wert deaktivieren**: Schaltet die automatische Anpassung der Größe des Programmfensters ab, wenn Sie hochauflösende Schriften verwenden. Programme, die größere Schriftarten verwenden, sehen ansonsten ziemlich merkwürdig aus.
- **Programm als Administrator ausführen**: Erlaubt die Ausführung des Programms mit Administratorrechten. Falls diese Option nicht angezeigt wird, müssen Sie sich als Administrator anmelden.
- **Aktivieren Sie dieses Programm, um mit One-Drive-Dateien zu arbeiten (Windows 8/8.1/10)**: Diese Option bietet Netzwerkunterstützung für ältere Anwendungen, die das Konzept der Cloud noch nicht kennen.
- **Einstellungen für alle Benutzer ändern**: Durch Anklicken dieser Schaltfläche werden die Kompatibilitätsanpassungen für alle Benutzer des Computers wirksam. Ansonsten gelten sie nur für den aktuellen Benutzer.

Hinweis

Im April 2014 hat Microsoft den offiziellen Support für Windows XP eingestellt. Das betrifft auch die virtuelle Maschine Windows-XP-Modus. Das System erhält also keine Sicherheitsupdates mehr. Verwenden Sie es mit Bedacht!

Es ist bestimmt kein Geheimnis mehr, dass Sie bei älteren Programmen versuchen sollten, diese im Kompatibilitätsmodus auszuführen, wenn sie unter neueren Windows-Versionen nicht oder nicht mehr korrekt laufen. Wenn Sie wirklich sorgfältig vorgehen wollen, suchen Sie erst im Web nach der Anwendung, bevor Sie diese auszuführen versuchen. Der Kompatibilitätsmodus ist ein praktisches Hilfsmittel, um ältere Anwendungen zum Laufen zu bringen.

16.3.4 Fehlende Datei oder ungültige Dateiversion

Manche Programme verlassen sich auf das Vorhandensein anderer Dateien, und das betrifft insbesondere DLLs. Einige Installationsprogramme bringen ihre eigenen DLLs mit und überschreiben die existierende Version. Später versuchen dann andere Programme, auf die ältere Version zuzugreifen und bekommen Probleme, wenn diese nicht gefunden werden kann.

Als Anwender sehen Sie in solchen Fällen dann eine Fehlermeldung wie »DLL fehlt« oder »Datei xyz konnte nicht geöffnet werden«. Dann ist es im Allgemeinen am einfachsten, das fragliche Programm erneut zu installieren und zu überprüfen, ob es bestimmte Dateiversionen benötigt. Wenn das nicht hilft, lässt sich dieses Problem für gewöhnlich durch eine Internetsuche nach der entsprechenden DLL und dem Namen des betreffenden Programms beheben.

16.3.5 Nicht reagierende Programme

Aus den verschiedensten Gründen kann es vorkommen, dass einige Standardprogramme in Windows oder im Microsoft Store gekaufte Apps nicht mehr funktionieren. Beispielsweise könnte eine Windows-Aktualisierung eine für die App wichtige Datei geändert haben.

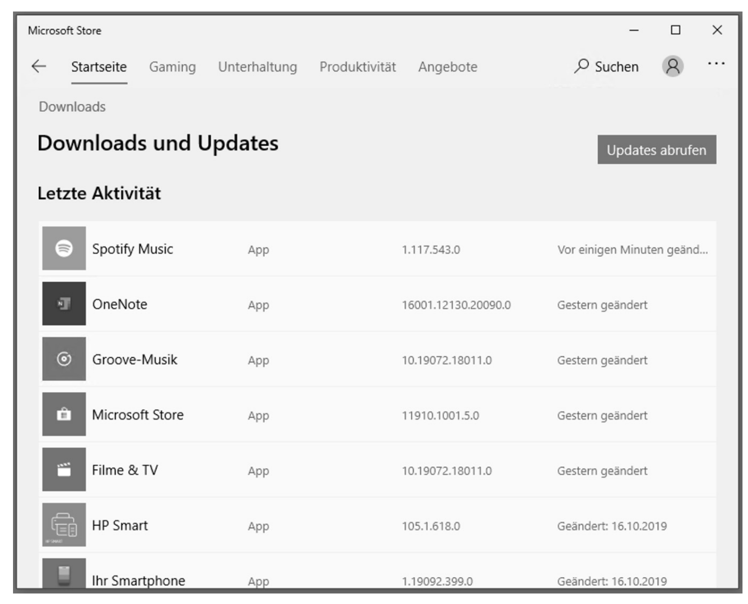


Abb. 16.48: Updates abrufen im Microsoft Store

Sie haben verschiedene Möglichkeiten, mit dieser Situation umzugehen. Besuchen Sie zunächst den Store und suchen Sie nach Updates für die problematische App (Abbildung 16.48). (Die Option wird angezeigt, wenn Sie auf die drei Punkte oben rechts klicken und DOWNLOADS UND UPDATES auswählen.) Halten Sie anschließend Ausschau nach einer Option, die App zu reparieren. Microsoft Edge bietet beispielsweise diese Möglichkeit.

Öffnen Sie EINSTELLUNGEN|APPS|APPS & FEATURES, wählen Sie MICROSOFT EDGE aus und klicken Sie auf ERWEITERTE OPTIONEN, um das Fenster in Abbildung 16.49 anzuzeigen. REPARIEREN versucht, Fehler zu beheben, lässt aber Ihre Daten und Konfiguration unangetastet. Wenn Sie ZURÜCKSETZEN auswählen, wird die von Ihnen vorgenommene Konfiguration gelöscht und Edge wird auf die Standardeinstellungen zurückgesetzt. Wählen Sie zuerst REPARIEREN aus. Wenn das nicht funktioniert, setzen Sie die App zurück.



Abb. 16.49: Die Optionen REPARIEREN und ZURÜCKSETZEN für Microsoft Edge in APPS & FEATURES

16.3.6 Abstürzende Programme

Hin und wieder erscheinen Programme, die eigentlich noch nicht reif für eine Veröffentlichung sind, und der fehleranfällige Code verursacht Programm- oder sogar Systemabstürze. Am häufigsten kommt dies bei Spielen vor, die übereilt veröffentlicht werden, um das Weihnachtsgeschäft nicht zu verpassen. Dieser hastig veröffentlichte Code führt mitunter zu spektakulären Resultaten. Sie sind mitten in einem spannenden Kampf mit dem Bösewicht und was passiert? Ein Programmabsturz und Sie finden sich auf dem Desktop wieder!

Miserabel programmierte oder fehleranfällige Programme können fürchterliche Folgen für Sie und Ihre Kunden haben. Solche Programme verursachen ein Einfrieren des Rechners oder spontane Neustarts. Diese unbeabsichtigten Abschaltungen können geöffnete Dateien in Mitleidenschaft ziehen und diese beschädigen.

Problematisch ist hier, dass die Ursache derartiger Abstürze auch die Hardware oder ein Gerätetreiber sein kann, nicht nur eine bestimmte Anwendung. All dies müssen Sie bedenken, wenn Sie sich auf die Suche nach den Gründen für die Abstürze begeben.

Betrachten wir ein typisches Szenario, in dem es vielfältige Ursachen für einen Absturz geben kann. Wenn beim Spielen eines grafisch anspruchsvollen Programms, das sehr viel Arbeitsspeicher bean-

sprucht, sowohl die Anwendung als auch Windows einfriert, was könnte dann der Grund dafür sein? Möglicherweise hat das Programm eine Betriebssystemroutine nicht korrekt aufgerufen, oder eine, die mit einer anderen Anwendung kollidiert. Eventuell ist die Grafikkarte an der Grenze ihrer Leistungsfähigkeit und wird einfach zu stark belastet. Vielleicht hat das System auch versucht, auf einen Bereich des Arbeitsspeichers zuzugreifen, der jetzt defekt ist.

Wenn unter denselben Umständen das Spiel zwar funktioniert, aber sich die Leistung des Systems insgesamt verschlechtert, welche Ursache käme dann infrage? Hier handelt es sich um einen Hinweis, der eher auf ein Problem der Anwendung als auf Hardware- oder Treiberprobleme hindeutet, insbesondere, wenn andere Programme einwandfrei laufen. Letztendlich läuft es darauf hinaus, dass Sie bei Abstürzen unvoreingenommen bleiben müssen und nichts ausschließen dürfen, ohne es vorher zu testen.

16.3.7 Volumeschattenkopie-Dienst und Computerschutz

Die größten Kopfschmerzen bei Anwendungsproblemen bereitet nicht die Anwendung selbst. Es sind vielmehr durch die Anwendung möglicherweise beschädigte Daten. Natürlich sind regelmäßige Sicherungen oder Wiederherstellungspunkte ein Ausweg, aber auch etwas mühsam. Falls Sie die Daten vorher nicht gesichert haben, besitzen Sie möglicherweise noch gar kein Backup. Microsoft hat sich mit dem *Computerschutz* für dieses Problem eine Lösung einfallen lassen.

Diese Funktion wird durch den *Volumeschattenkopie-Dienst* (*VSS – Volume Shadow Copy Service*) bereitgestellt, der es dem Betriebssystem ermöglicht, Sicherheitskopien aller Dateien zu erstellen, selbst wenn diese in Gebrauch sind. In Windows wird der Volumeschattenkopie-Dienst auch vom Computerschutz verwendet, der es Ihnen erlaubt, auf vorherige Versionen von Dateien und Ordnern zuzugreifen. Klicken Sie mit der rechten Maustaste auf eine Datendatei und wählen Sie VORGÄNGERVERSIONEN WIEDERHERSTELLEN aus, wodurch das EIGENSCHAFTEN-Dialogfeld mit ausgewählter Registerkarte VORGÄNGERVERSIONEN geöffnet wird (Abbildung 16.50).

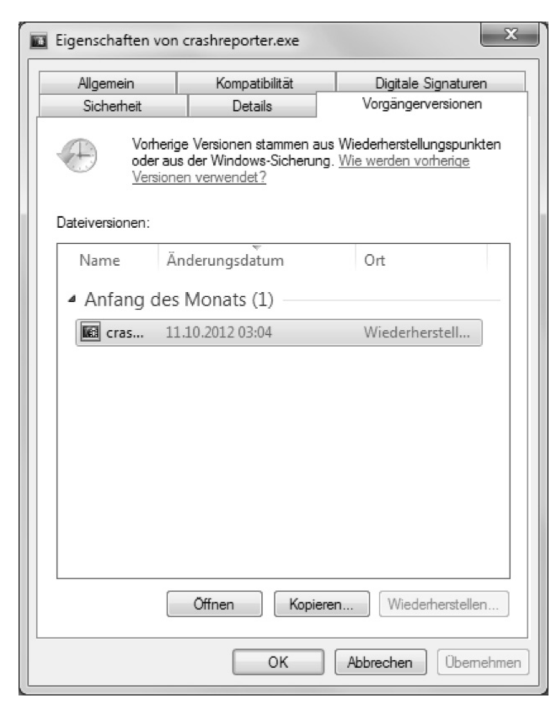


Abb. 16.50: Die Registerkarte VORGÄNGERVERSIONEN

Hinweis

Aus ungeklärten Gründen hat Microsoft die Registerkarte VORGÄNGERVERSIONEN für lokale Volumes aus Windows 8/8.1 entfernt, in Windows 10 ist sie hingegen wieder vorhanden. Wenn Sie in Windows 8/8.1 einzelne Dateien wiederherstellen möchten, können Sie das Applet DATEIVERSIONSVERLAUF in der Systemsteuerung verwenden, das Sie in Kapitel 14 kennengelernt haben. Vergessen Sie nur nicht, es rechtzeitig einzurichten!

Wenn eines der nachstehenden Kriterien erfüllt ist, wird in der Liste mindestens eine Vorgängerversion angezeigt:

- Die Datei oder der Ordner wurde mit dem Sicherungsprogramm gesichert.
- Sie haben einen Wiederherstellungspunkt angelegt.
- Die Datei oder der Ordner wurde geändert.

Natürlich müssen Sie außerdem auch den COMPUTERSCHUTZ aktiviert haben. Öffnen Sie das Dialogfeld SYSTEMEIGENSCHAFTEN und wählen Sie die Registerkarte COMPUTERSCHUTZ aus (Abbildung 16.51), um anzuzeigen, ob die Funktion aktiviert ist. (Standardmäßig sollte dies der Fall sein.)



Abb. 16.51: Die Registerkarte COMPUTERSCHUTZ

Hinweis

Beachten Sie, dass der COMPUTERSCHUTZ nicht nur beim Wiederherstellen durch defekte Anwendungen beschädigter Datendateien von Nutzen ist. Sie können ihn auch zum Wiederherstellen versehentlich überschriebener Dateien verwenden. Auf der Registerkarte COMPUTERSCHUTZ steht außerdem praktischerweise die Möglichkeit zur Verfügung, einen Wiederherstellungspunkt zu erstellen oder zu laden.

Der COMPUTERSCHUTZ gehört zur Kategorie Dateiwiederherstellungs-Software und erledigt seine Aufgabe ausgezeichnet. Es gibt ähnliche Software von Drittanbietern, wie beispielsweise *Recuva* von Piriform, das ich viele Male dazu verwendet habe, »gelöschte« Dateien auf Festplatten oder Laufwerken mit Flash-Speicher (wie USB-Speichersticks) wiederherzustellen.

16.4 Wiederholung

16.4.1 Fragen

1. Welches Werkzeug hilft Ihnen dabei, das Programm zu identifizieren, das den Prozessor so sehr in Beschlag nimmt?
   A. TASK-MANAGER
   B. GERÄTE-MANAGER
   C. WARTUNGSCENTER
   D. SYSTEMINFORMATIONEN
2. Welches Werkzeug gestattet es, den Zustand eines Windows-Systems zu einem früheren Zeitpunkt wiederherzustellen?
   A. Systemkonfigurationsprogramm
   B. Snapshot-Manager
   C. Systemwiederherstellung
   D. GRUB oder LILO
3. Richards Computer mit Windows 10 arbeitet nicht mehr so schnell wie früher. Welche Option sollte er wählen, um sein System zurückzusetzen, ohne dabei persönliche Daten und Einstellungen zu löschen?
   A. PC auffrischen
   B. Originaleinstellung wiederherstellen
   C. ERWEITERTE OPTIONEN|SYSTEMWIEDERHERSTELLUNG
   D. System auffrischen
4. Was können fehlerhafte Gerätetreiber und defekte Hardware in macOS und Linux auslösen?
   A. Ein sich drehendes regenbogenfarbiges Scheibchen (Pinwheel of Death)
   B. Blue Screen of Death (BSoD)
   C. Kernel Panic
   D. Terminalemulation
5. Welcher der folgenden Punkte weist eher auf ein Hardware- oder CMOS-Problem als auf ein Problem mit dem Betriebssystem hin, wenn ein PC nicht startet?
   A. Schwarzer Bildschirm mit der Fehlermeldung `Ungültiges Startlaufwerk`
   B. Schwarzer Bildschirm mit der Fehlermeldung `NTLDR fehlerhaft oder nicht vorhanden`
   C. Schwarzer Bildschirm mit der Fehlermeldung `BOOT.INI nicht vorhanden`
   D. Schwarzer Bildschirm mit der Fehlermeldung `BCD ungültig`
6. Wolfgangs Computer zeigt eine Fehlermeldung, die besagt, dass `bootmgr` defekt ist. Mit welchem Werkzeug lässt sich das Problem beheben?
   A. `bcdedit`
   B. `chkdsk`
   C. `diskpart`
   D. `regedit`
7. Wie bezeichnet Microsoft die 32- oder 64-Bit-Installationsumgebung in Windows?
   A. WinEE
   B. WinPE
   C. WinRE
   D. WinVM

8. Ralph vermutet, dass ein defektes RAM-Speichermodul Schuld daran ist, dass Windows nicht startet. Mit welchem Windows-Standardwerkzeug kann er das RAM überprüfen?
   A. MEMMAKER
   B. Memtest86+
   C. Windows-RAM-Diagnosetool
   D. Windows-Speicherdiagnose
9. Welches der folgenden Kommandos repariert einen defekten Master Boot Record auf einem PC mit Windows 10?
   A. `bootrec /fixboot`
   B. `bootrec /fixmbr`
   C. `fixboot`
   D. `fixmbr`
10. Welche Funktion in Windows 7 und 10 ermöglicht es Ihnen, eine Datei oder einen Ordner mit der rechten Maustaste anzuklicken und Vorgängerversionen davon wiederherzustellen?
   A. SYSTEMWIEDERHERSTELLUNGSOPTIONEN
   B. COMPUTERSCHUTZ
   C. DATEIVERSIONSVERLAUF
   D. WIEDERHERSTELLUNG

16.4.2 Antworten

1. **A.** Ein Programm, das den Prozessor in Beschlag nimmt, kann der Task-Manager sehr schnell identifizieren.
2. **C.** Die SYSTEMWIEDERHERSTELLUNG verwendet *Wiederherstellungspunkte* (Momentaufnahmen des Systems zu einem bestimmten Zeitpunkt), um das System auf einen vorhergehenden Zustand zurückzusetzen.
3. **A.** In Windows 10 können Sie mit der Option PC AUFFRISCHEN den PC zurücksetzen, die Daten und Einstellungen bleiben dabei jedoch erhalten. Die Option ORIGINALEINSTELLUNG WIEDERHERSTELLEN löscht hingegen die Daten und Sie finden ein frisch installiertes Windows vor.
4. **C.** Fehlerhafte Gerätetreiber und defekte Hardware können in macOS und Linux eine Kernel Panic verursachen und das ganze System zum Absturz bringen.
5. **A.** Bei einem PC, der nicht startet, weist ein schwarzer Bildschirm mit der Fehlermeldung `Ungültiges Startlaufwerk` auf ein Problem mit der Hardware oder der CMOS-Konfiguration hin.
6. **A.** Ein defekter `bootmgr` kann mit `bcdedit` repariert werden.
7. **B.** Microsoft bezeichnet die 32- oder 64-Bit-Installationsumgebung als *Windows-Vorinstallationsumgebung* (*WinPE – Windows Preinstallation Environment*).
8. **D.** Ralph sollte die Windows-Speicherdiagnose zur Überprüfung des RAMs verwenden.
9. **B.** Führen Sie unter Windows 10 in WinRE das Kommando `bootrec /fixmbr` aus, um einen defekten Master Boot Record zu reparieren.
10. **B.** In Windows 7 und 10 ermöglicht Ihnen die Funktion COMPUTERSCHUTZ, ein Objekt mit der rechten Maustaste anzuklicken und Vorgängerversionen wiederherzustellen.

Anzeige: Bildschirm und Grafikkarte | 17

Themen in diesem Kapitel:

- Funktionsweise der Bildschirmanzeige
- Auswahl der richtigen Grafikkarte
- Bildschirmtreiber installieren und konfigurieren
- Fehlersuche bei grundlegenden Anzeigeproblemen

Die Begriffe *Anzeige* und *Grafiksystem* beziehen sich auf das komplexe Zusammenspiel zwischen zahlreichen PC-Komponenten, die gemeinsam Bilder auf einem Monitor anzeigen. Der Monitor zeigt an, was Programme und das Betriebssystem gerade machen, und ist das primäre Ausgabegerät der meisten Rechner. Die *Grafikkarte* bzw. der *Grafikadapter* ist für die gesamte Kommunikation zwischen der CPU und dem Monitor zuständig (Abbildung 17.1). Das Betriebssystem muss wissen, wie es mit der Kommunikation zwischen der CPU und der Grafikkarte umgehen muss, weshalb es auf für die jeweiligen Grafikkarten spezifische Treiber und die passenden Einstellungen des Betriebssystems angewiesen ist. Schließlich müssen alle Anwendungen mit dem übrigen Grafiksystem zusammenarbeiten können. Die dafür verantwortlichen Komponenten gehören in die Kategorie Anzeigetechnologie. In diesem Kapitel werden wir die vier Arten dieser Komponenten eingehend betrachten und abschließend die Fehlerbehebung bei Problemen mit der Anzeige behandeln.

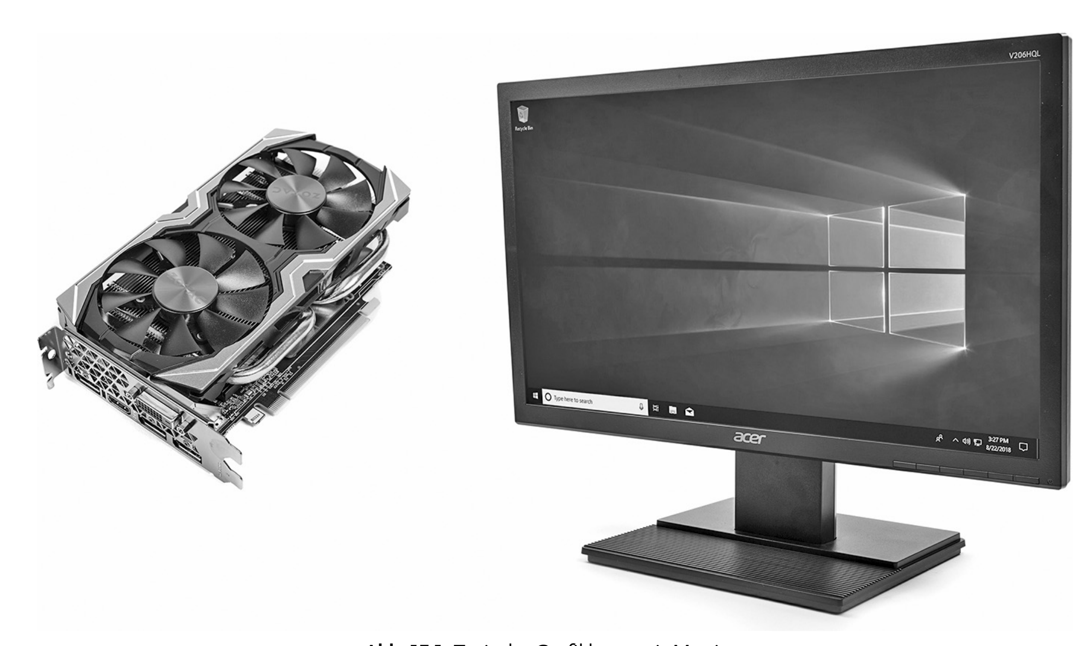


Abb. 17.1: Typische Grafikkarte mit Monitor

17.1 Grafikanzeige

Grafikanzeigen für PCs gibt es in drei Varianten: LCD, Projektoren und Headsets (zur Anzeige einer virtuellen Realität). Heutzutage verwenden fast alle PCs einen LCD-Bildschirm; Projektoren findet man vor allem in Konferenzräumen und Klassenzimmern, wo Bilder an die Wand geworfen werden. Bei einem Headset befinden sich zwei gleichartige Displays nebeneinander. In diesem Abschnitt befassen ich mich mit den verschiedenen Technologien und erörtere die Anschlussmöglichkeiten.

Wichtig

PCs und Macs verwendeten ursprünglich Röhrenmonitore, große und klobige Geräte. Röhrenmonitore gehören der Vergangenheit an, sie tauchen jedoch in der CompTIA-Zertifizierungsprüfung in einer Frage zur Entsorgung giftiger Abfälle auf. Röhrenmonitore enthalten giftige Bestandteile, deshalb müssen sie fachgerecht entsorgt werden und dürfen keinesfalls in den normalen Hausmüll gegeben werden.

17.1.1 LCD-Bildschirme

Fast alle aktuellen Computer und computerartigen Geräte verwenden LCD-Bildschirme (*Liquid Crystal Displays*). Sie können sich sicher vorstellen, dass es in Anbetracht der Unzahl verschiedener Computer auch eine enorme Bandbreite verschiedener LCD-Bildschirme gibt. Sehen wir uns zunächst einmal die Technologie und dann einige der Varianten an.

Geschichte und Konzepte

Die Funktionsweise von LCDs

Wenn man LCDs verstehen will, muss man das Konzept der Polarität des Lichts kennen. Wer in der Schule schon einmal mit einem Prisma gespielt oder einen Regenbogen betrachtet hat, weiß, dass sich das Licht in Form von Wellen fortbewegt (hier bitte keine Quantenmechanik) und dass die Wellenlänge die Farbe des Lichts bestimmt. Weniger bekannt ist, dass die Lichtwellen in drei Dimensionen von einer Lichtquelle abgestrahlt werden. Da sich ein Diagramm dreidimensionaler Wellen nicht abdrucken lässt, verwenden wir stattdessen eine Analogie. Denken Sie, um sich das Ganze besser vorstellen zu können, an das von einer Taschenlampe abgestrahlte Licht. Stellen Sie sich nun das von der Taschenlampe abgestrahlte Licht als Springseil vor, das von jemandem bewegt wird. Dabei handelt es sich nicht etwa um ein rhythmisches Schwingen (vor und zurück oder auf und ab), sondern eher um wilde Bewegungen in unterschiedlicher Geschwindigkeit, mit denen das Seil kreuz und quer über den ganzen Platz geschwungen wird (auf und ab, rechts und links mit ständig wechselnder Geschwindigkeit).

So verhält sich Licht. Treiben wir die Analogie noch ein wenig weiter und nehmen wir an, dass die Person unendlich viele Arme hat, mit denen sie jeweils ein Springseil in alle denkbaren Richtungen schwingt, um uns so die »Dreidimensionalität« der Lichtwellen vorzustellen. Leider kann ich das (a) nicht zeichnen und (b) reicht ein Springseil durchaus zur Erklärung von LCDs aus. Die verschiedenen Geschwindigkeiten sorgen für unterschiedliche Wellenlängen (von sehr kurz bis sehr lang). Wenn Licht mit vielen verschiedenen Wellenlängen von unseren Augen aufgenommen wird, sehen wir weißes Licht. Wenn das Licht lediglich eine Wellenlänge hat, sehen wir nur diese Farbe. Licht, das durch einen polarisierenden Filter gelenkt wird (wie z.B. eine Sonnenbrille), lässt sich mit einem Gartenzaun mit senkrechten Latten vergleichen, der sich zwischen uns und der Person befindet, die das Springseil schwingt. Wir sehen zwar alle Wellenlängen, aber nur die Wellen mit ähnlicher Ausrichtung. Wir würden immer noch alle Farben sehen, allerdings sähen wir diese schwächer, weil wir nur die Wellen mit derselben Ausrichtung sehen könnten, wodurch das Bild dunkler wäre. Aus diesem Grunde verwenden viele Sonnenbrillen Polarisationsfilter.

Was würde nun passieren, wenn wir einen weiteren Gartenzaun verwenden würden, bei dem die Zaunlatten horizontal verlaufen? Das würde dazu führen, dass letztlich alle Wellen eliminiert werden. Das ist dann der Fall, wenn zwei polarisierende Filter in einem 90-Grad-Winkel kombiniert werden: Es wird kein Licht mehr durchgelassen.

Was würde nun passieren, wenn zwischen die beiden Zäune ein dritter Zaun eingefügt wird, bei dem die Latten in einem 45-Grad-Winkel angeordnet sind? Dies würde dafür sorgen, dass einige der Schwingungen des Seils so umgelenkt werden, dass die Wellen durchgelassen werden. Dasselbe gilt für polarisierende Filter. Der dritte Filter lenkt einen Teil des Lichts so ab, dass es durchgelassen wird. Sollten Sie wissenschaftlich ambitioniert sein, können Sie sich im Lehrmittelhandel für ein paar Euro drei polarisierende Filter besorgen und es selbst ausprobieren. Es funktioniert wirklich.

Flüssigkristalle nutzen die Eigenschaften der Polarisierung aus. Flüssigkristalle bestehen aus einer speziell beschaffenen Flüssigkeit, in der lange, dünne Kristalle enthalten sind, die sich ständig selbst in derselben Richtung auszurichten versuchen (Abbildung 17.2). Diese Substanz verhält sich genau wie ein flüssiger polarisierender Filter. Wenn man eine dünne Schicht von diesem Zeug zwischen zwei kleine Glasscheibchen gießen würde, hätte man eine verdammt gute Sonnenbrille.

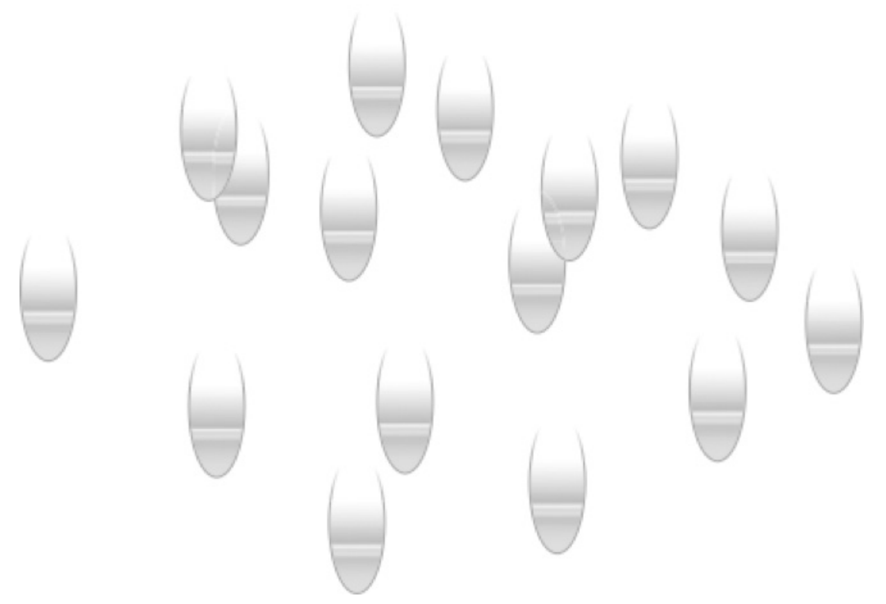


Abb. 17.2: Wellen gleicher Ausrichtung

Stellen Sie sich vor, man würde extrem feine Rillen auf einer Seite dieser Glasscheibchen einritzen. Wenn Sie diese Flüssigkeit mit einer fein gerillten Oberfläche in Kontakt bringen, dann richten sich die Moleküle selbstständig nach den Rillen in der Oberfläche aus (Abbildung 17.3).

Wenn man nun eine weitere fein gerillte Oberfläche hinzufügt, deren Rillen in einem 90-Grad-Winkel zur anderen Oberfläche ausgerichtet sind und die der anderen Oberfläche gegenüberliegt, dann versuchen die Moleküle, die zu dieser Seite Kontakt haben, sich nach deren Rillen auszurichten. Die Moleküle dazwischen richten sich im Bestreben, sich an beiden Flächen zu orientieren, sofort in einer netten Drehung aus (Abbildung 17.4). Wenn dann zwei rechtwinklige polarisierende Filter auf die beiden Seiten der Flüssigkristalle platziert werden, lenken die Flüssigkristalle das Licht so ab, dass es durchgelassen wird (Abbildung 17.5).

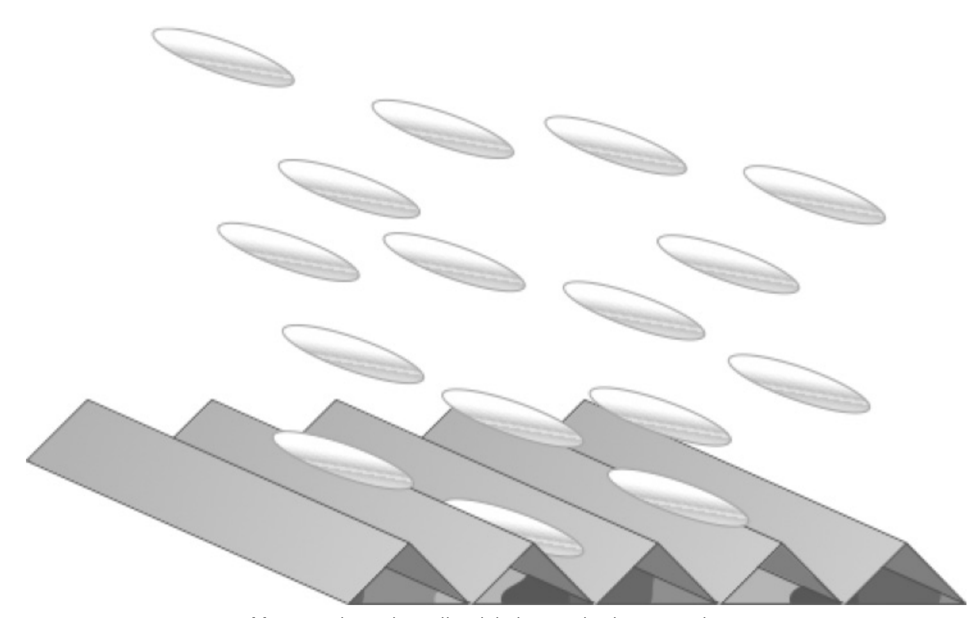


Abb. 17.3: Flüssigkristallmoleküle mit gleicher Ausrichtung

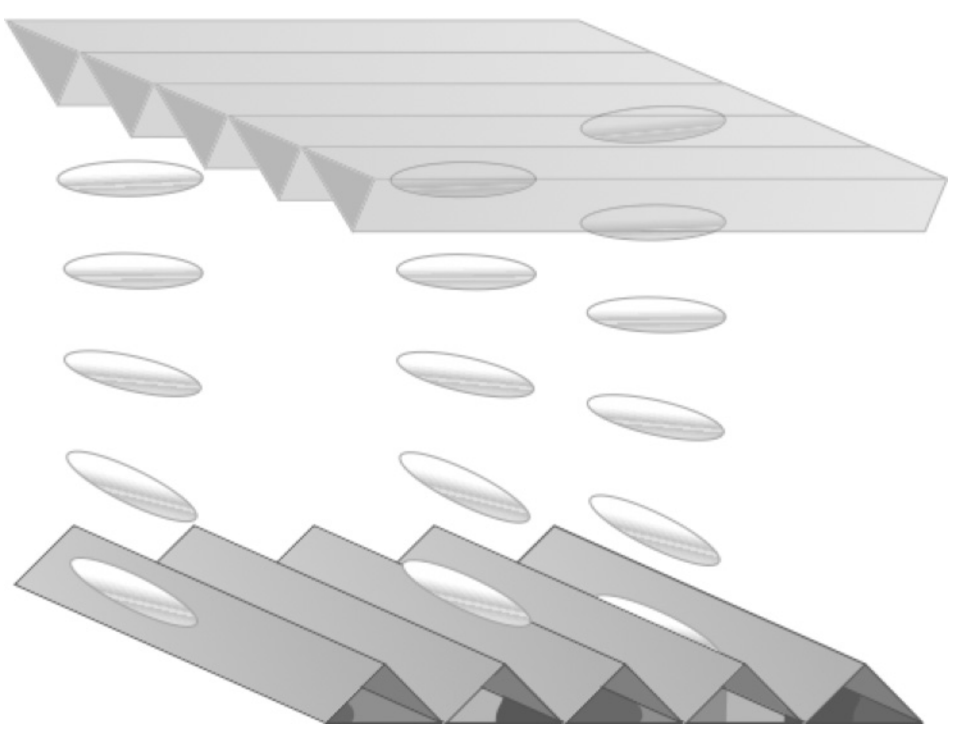


Abb. 17.4: Flüssigkristallmoleküle versuchen, sich auszurichten.

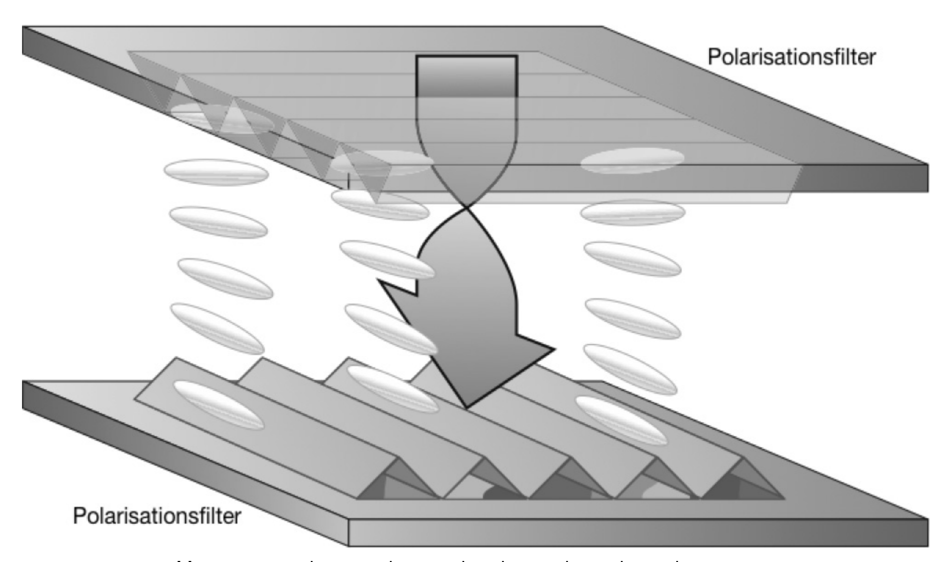


Abb. 17.5: Wenn keine Ladung vorhanden ist, kann das Licht passieren.

Wenn man an die Flüssigkristalle nun ein elektrisches Potenzial anlegt, dann ändern die Kristalle ihre Ausrichtung und passen sich an die Richtung des elektrischen Feldes an. Die Drehung verschwindet und es wird kein Licht mehr durchgelassen (Abbildung 17.6).

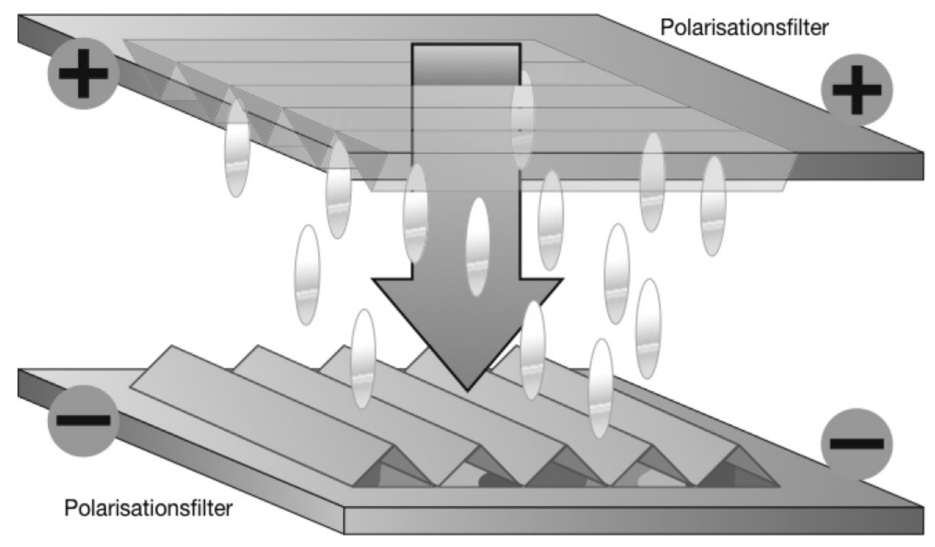


Abb. 17.6: Sind elektrische Ladungen vorhanden, wird kein Licht mehr durchgelassen.

1001

Ein LCD-Farbbildschirm setzt sich aus einer großen Anzahl winziger Flüssigkristallmoleküle (sogenannter *Subpixel*) zusammen, die zwischen polarisierenden Filtern in Reihen und Spalten angeordnet sind. Eine lichtdurchlässige Folie oberhalb der Subpixel ist rot, grün oder blau eingefärbt. Jede win-

zige, aus drei Subpixeln – einem roten, einem grünen und einem blauen – bestehende Einzelgruppe bildet ein physisches Pixel, wie in Abbildung 17.7 gezeigt.

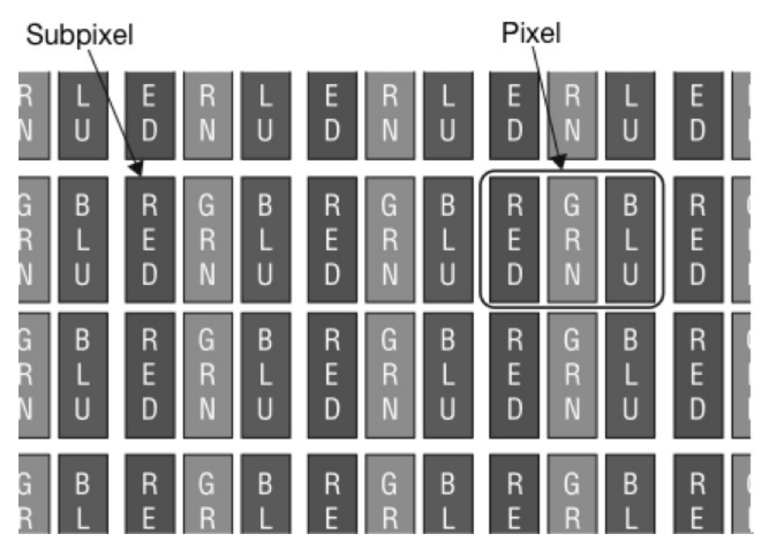


Abb. 17.7: LCD-Pixel

Wie aber könnte man, nachdem alle Pixel an Ort und Stelle sind, die jeweils richtigen Positionen laden, um ein Bild zu erzeugen? Die früheren LCDs verwendeten keine rechteckigen Pixel. Stattdessen setzten sich die Bilder aus unterschiedlich geformten Elementen zusammen, die alle elektrisch voneinander getrennt waren. Um ein Bild zu erzeugen, wurden die jeweils benötigten Bereiche gleichzeitig geladen. Abbildung 17.8 zeigt die Zahl 0. Diese Anzeige ist möglich, wenn sechs Bereiche geladen werden, die eine Art Ellipse bilden. Dieser Prozess, die sogenannte *statische Ladung*, wird in vielen einfachen Ziffernanzeigen (z.B. bei Taschenrechnern) immer noch verwendet.

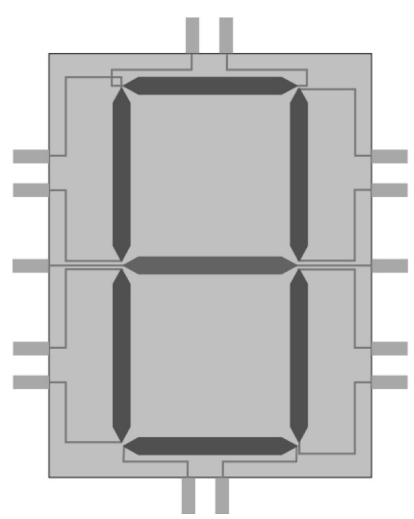


Abb. 17.8: Einzelnes Zeichen auf einem statischen numerischen LCD

Das statische Verfahren lässt sich wegen seiner geringen Flexibilität beim PC nicht einsetzen. Stattdessen wurde bei der ersten Generation der LCD-Bildschirme für den PC ein Gitter aus Drähten eingesetzt (Abbildung 17.9). Die vertikalen Drähte (Y-Drähte) verlaufen zu jedem einzelnen Subpixel in der Spalte. Die horizontalen Drähte (X-Drähte) sind mit einer ganzen Reihe von Subpixeln verbunden. Sowohl der X- als auch der Y-Draht müssen geladen sein, damit genügend Spannung aufgebaut wird, um ein einzelnes Subpixel zum Leuchten zu bringen.

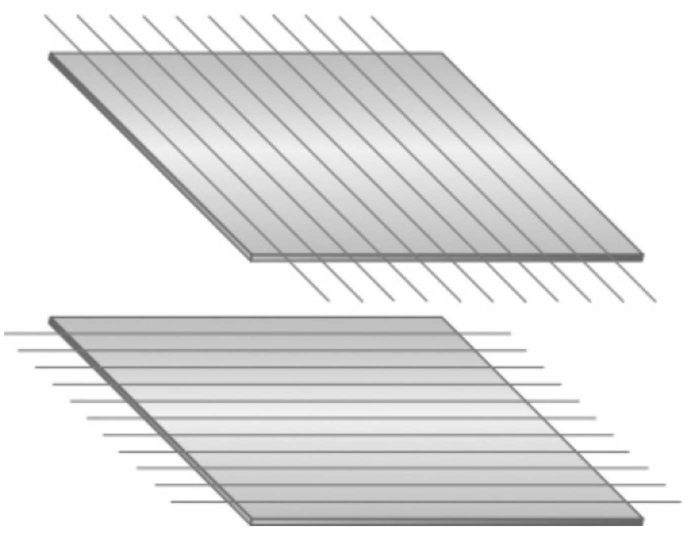


Abb. 17.9: LCD-Matrix aus Drähten

Wenn Farben angezeigt werden sollen, benötigt man drei Matrizen. Die drei Matrizen überschneiden sich und liegen dabei sehr dicht beieinander. Über den Schnittpunkten ist das Glas mit winzigen roten, grünen und blauen Punkten bedeckt. Durch unterschiedlich starke Spannungspegel lassen sich Rot, Grün und Blau in unterschiedlicher Intensität erzeugen (Abbildung 17.10). Diese Technologie wird Passiv-Matrix-LCD genannt.

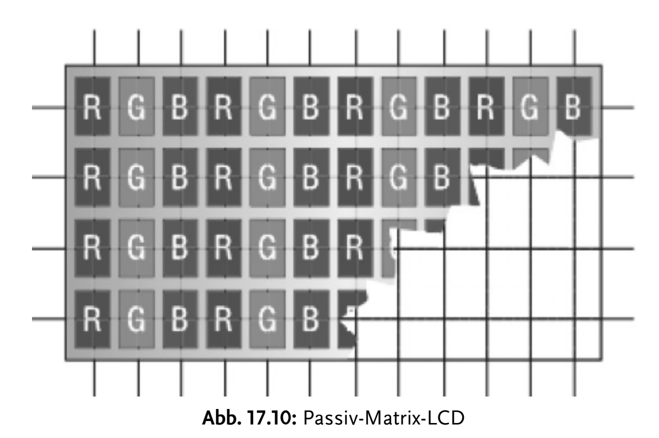


Abb. 17.10: Passiv-Matrix-LCD

Heutige LCD-Bildschirme verwenden eine sogenannte *Aktiv-Matrix* mit TFTs (Thin Film Transistor) (Abbildung 17.11). Statt X- und Y-Drähten werden ein oder mehrere winzige Transistoren zur Steuerung der einzelnen Farbpunkte verwendet, wodurch eine schnellere Bildanzeige, eine klarere Pixelabgrenzung und eine sehr viel genauere Farbkontrolle als bei älteren Technologien möglich werden.

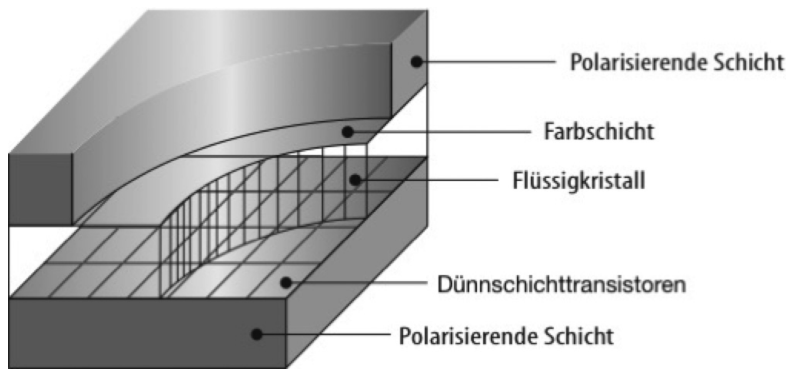


Abb. 17.11: Aktiv-Matrix (TFT)

LCD-Bauteile

Der typische LCD-Monitor setzt sich aus zwei oder drei Komponenten zusammen: dem LCD-Panel, der Hintergrundbeleuchtung und (in älteren Modellen) den Invertern. Das LCD-Panel erzeugt das Bild, die Hintergrundbeleuchtung beleuchtet das Bild, damit Sie es sehen, und die Inverter versorgen die Hintergrundbeleuchtung mit Strom, wenn diese eine Wechselspannung benötigen. Abbildung 17.12 zeigt die typische Anordnung der internen Komponenten eines älteren LCD-Bildschirms.

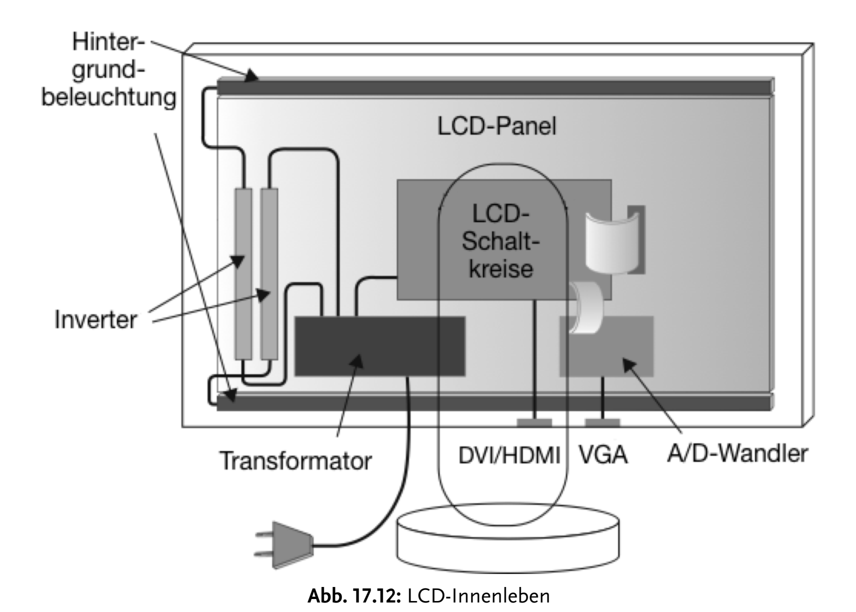


Abb. 17.12: LCD-Innenleben

LCD-Technologien Die Hersteller von LCD-Bildschirmen verwenden viele Varianten bei Dingen wie der Ausrichtung der Flüssigkristallmoleküle im Glassubstrat und der Steuerelektronik, um Displays mit schnellen Reaktionszeiten und natürlicher Farbdarstellung anbieten zu können. Die drei heutzutage verbreitetsten Technologien sind *Twisted Nematic* (TN), das sogenannte *In-Plane-Switching* (*IPS*) und Vertical Alignment (VA). TN-Bildschirme sind im Allgemeinen am schnellsten, bieten aber nur eine mäßige Farbdarstellung. IPS-Bildschirme stellen Farben sehr naturgetreu dar. VA-Displays liegen in beiden Bereichen irgendwo dazwischen. Um diese Unterschiede zu verstehen (was für die Zertifizierungsprüfung erforderlich ist), müssen wir uns ausführlich ansehen, wie die verschiedenen

Merkmale der Monitore funktionieren. Zunächst betrachten wir die Hintergrundbeleuchtung und anschließend die verschiedenen Features. Am Ende des Kapitels vergleichen wir die drei wichtigsten Technologien miteinander.

Hinweis

Samsung bietet eine eigene IPS-Version namens PLS (Plane to Line Switching) an. Das Unternehmen behauptet (natürlich), dass sie der normalen IPS-Version überlegen sei, allerdings funktioniert sie sehr ähnlich und kann durchaus als IPS-Variante betrachtet werden.

Hintergrundbeleuchtung Die Hintergrundbeleuchtung beleuchtet das LCD-Panel. Zu diesem Zweck werden jedoch verschiedene Technologien und Implementierungen eingesetzt. Aktuelle LCD-Bildschirme verwenden LEDs für die Hintergrundbeleuchtung, während frühere Generationen Kaltkathodenlampen verwendeten. Die modernen Monitore werden unter der Bezeichnung LED-Display vermarktet, um sie von Bildschirmen mit Kaltkathodenlampen abzugrenzen. LEDs haben Kaltkathodenlampen verdrängt, weil LEDs ebenso wie die LCD-Schaltkreise und das LCD-Panel mit Gleichstrom arbeiten. Sie verbrauchen deutlich weniger Energie und geben keine Wärme ab. LEDs ermöglichen extrem flache Bildschirme, wie man heute an fast allen Computer-ähnlichen Geräten sieht – vom Smartphone über Tablets bis hin zu Monitoren für Desktop-PCs. Abbildung 17.13 zeigt den Aufbau eines typischen modernen LCD-Displays. Beachten Sie, dass es die Inverter (vgl. Abbildung 17.12) nicht mehr gibt.

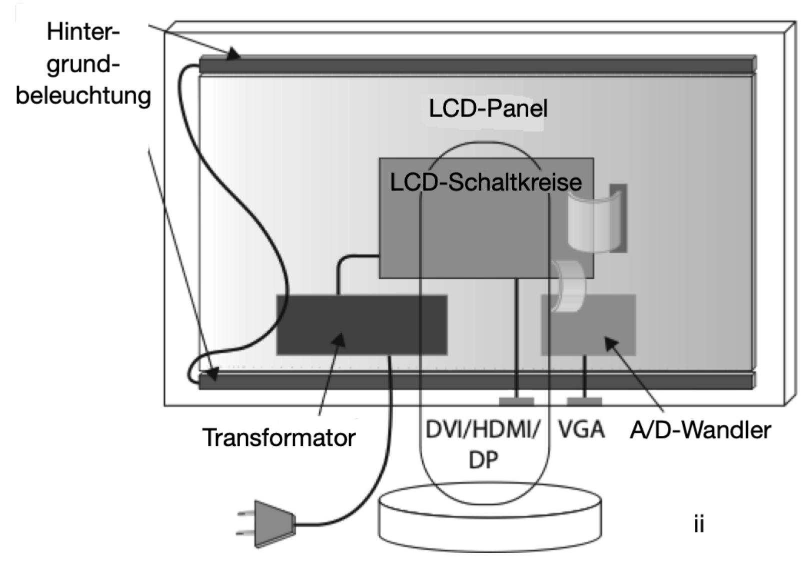


Abb. 17.13: Innenleben eines modernen LCD-Displays

Beachten Sie in Abbildung 17.12, dass dieser Bildschirm zwei Hintergrundbeleuchtungen verwendet: eine oben und eine unten. Dieser Aufbau ist typisch für Hintergrundbeleuchtungen, hat aber den Nachteil, dass manchmal die Ränder etwas heller erscheinen als die Bildschirmmitte.

Bei einer direkten LED-Hintergrundbeleuchtung befindet sich eine Reihe von LEDs hinter dem LCD-Panel, wodurch eine bessere, gleichförmigere Ausleuchtung erreicht wird. Diese Technologie ist teurer als die Ausleuchtung vom Rand aus und benötigt auch mehr Energie, wird jedoch bei hochwertigen LCD-Fernsehern und Computerbildschirmen immer gebräuchlicher.

Die ersten LCD-Bildschirme verwendeten für die Hintergrundbeleuchtung *Kaltkathodenlampen* (*CCFL – Cold Cathode Florescent Lamp*), die für einen geringen Energiebedarf, gleichmäßige Ausleuchtung und lange Lebensdauer bekannt sind. Abbildung 17.14 zeigt eine Kaltkathodenlampe aus einem LCD-Panel. Kaltkathodenlampen benötigen für ihren Betrieb hochfrequenten Wechselstrom, was es erforderlich machte, einen Inverter zu verwenden, der den Gleichstrom des Transformators wieder in Wechselstrom umwandelt. Deshalb waren die Panels früher deutlich dicker als heutzutage. Monitore mit Kaltkathodenlampen sind noch immer in Gebrauch, allerdings ist es ratsam, sie zu ersetzen, wenn irgendwelche Bauteile einen Defekt aufweisen, statt zu versuchen, sie zu reparieren, denn moderne Monitore sind ihnen in allen Belangen überlegen.



Abb. 17.14: Kaltkathodenlampe

17.1.2 LCD-Varianten

LCDs unterscheiden sich in vielerlei Hinsicht, und kompetente Techniker müssen diese Unterschiede kennen, um einen geeigneten Monitor für die Bedürfnisse ihrer Kunden zu finden. Damit ich beim Thema bleibe, konzentrieren ich mich auf die Merkmale, die in der Zertifizierungsprüfung 1001 vorkommen (wie Auflösung und Farbtiefe). Die Prüfung greift bei modernen LCD-Varianten etwas kurz, deshalb habe ich im Abschnitt *Jenseits von A+* Informationen darüber hinzugefügt, was die Bemühungen der Hersteller betrifft, Bildschirme zu bauen, die anzeigen, was das menschliche Auge wahrnehmen kann. Der Bildschirm ist bei den meisten Computern das wichtigste Ausgabegerät, deshalb dürfte er wohl größere Bedeutung haben als alle anderen Bestandteile eines Computersystems. Ich werde die folgenden Themen erörtern:

- Auflösung
- Helligkeit
- Blickwinkelabhängigkeit
- Reaktionszeit
- Bildwiederholrate
- Kontrastverhältnis
- Farbtiefe

Auflösung

Alle LCD-Monitore haben eine natürliche (native) Auflösung, wie z.B. 2.560 x 1.440, bei der sie ihr schärfstes Bild liefern. Mehr als die natürliche Auflösung ist mit LCDs nicht möglich, und wenn man sie mit einer geringeren als der natürlichen Auflösung betreibt, wird die Darstellungsqualität deutlich schlechter. Wenn eine geringere als die natürliche Auflösung verwendet wird, müssen bei LCDs Kantenglättungsverfahren (Anti-Aliasing) eingesetzt werden, um den Treppeneffekt an den Rändern der Pixel abzuschwächen, was zu einer mehr oder weniger deutlich schlechteren Darstellungsqualität führt. Und das Fazit? Nutzen Sie bei LCDs einfach immer deren Maximalauflösung!

Hinweis

Zwei LCD-Bildschirme mit denselben physischen Abmessungen können sehr wohl unterschiedliche natürliche Auflösungen besitzen.

Für manche der nativen Auflösungen gibt es Bezeichnungen, die man gelegentlich in der Werbung sieht. Sie reichen von der uralten Auflösung von 640 x 480 (VGA) bis zur Auflösung von 1.366 x 768 (WXGA), die viele Bildschirme von preiswerten 15-Zoll-Laptops besitzen. Für die typische Auflösung von 1.920 x 1.080, die viele Monitore aufweisen, gibt es zwei Bezeichnungen: *FHD* (das steht für *Full High Definition*) oder *1080p*. Im Abschnitt *Jenseits von A+* finden Sie eine Tabelle, die Ihre Neugier zufriedenstellt. In der Prüfung findet sich lediglich die VGA-Auflösung im Bereich Problembehandlung (mehr dazu in Kürze).

Die Anordnung der Pixel auf dem Bildschirm legen das *Bildseitenverhältnis* fest, wie etwa 16:9 oder 21:9 (Abbildung 17.15). Ein typischer Breitbildschirm mit 1.920 x 1.080 Pixeln ist ein Beispiel für ein Bildseitenverhältnis von 16:9. Ein Bildschirm an einem Arbeitsplatzrechner zur Videobearbeitung mit 3.440 x 1.440 Pixeln ist ein Beispiel für ein Bildseitenverhältnis von 21:9. Bei vielen Monitoren lässt sich das Bildseitenverhältnis ändern, in Windows beispielsweise in EINSTELLUNGEN|ANZEIGE, aber die Qualität der Darstellung leidet darunter.

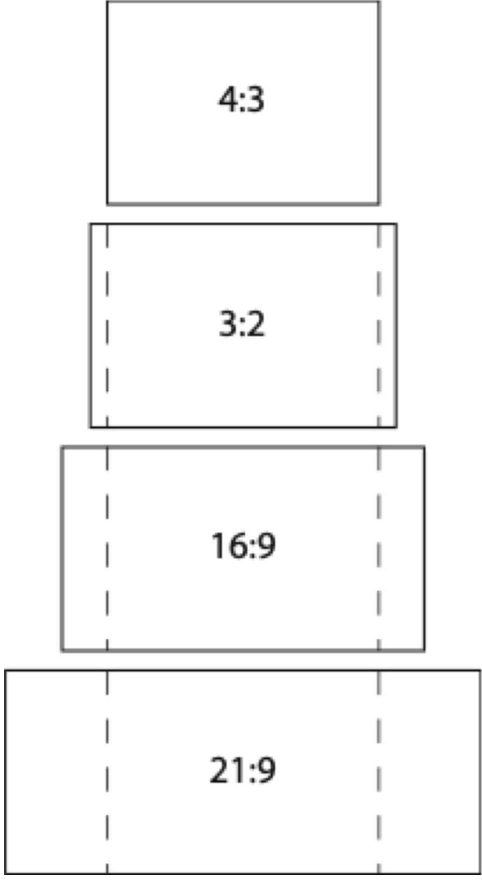


Abb. 17.15: Vergleich der Bildseitenverhältnisse

Moderne Geräte verwenden unterschiedliche Bildseitenverhältnisse. Die meisten Smartphones sind bei 16:9 geblieben, aber viele neuere Android- und iPhone-Modelle verwenden breitere Seitenverhältnisse wie 18:9 oder 19,5:9. Die meisten iPads verwenden hingegen ein Seitenverhältnis von 4:3. Microsofts Surface-Laptops verwenden ein Bildseitenverhältnis von 3:2.

Hinweis: PPI

Auflösung und physische Abmessungen eines Bildschirms legen den PPI-Wert (Pixels Per Inch) eines Bildschirms fest. Je größer dieser Wert ist, desto schärfer ist das Bild, das der Monitor darstellen kann. Das bedeutet in der Praxis, dass ein kleiner hochauflösender Monitor ein besseres Bild liefert als ein großer Bildschirm mit der gleichen Auflösung. Die Darstellung auf einem 24 Zoll großen 1080p-Monitor sieht beispielsweise bei knapp 100 PPI gut aus. Das Bild auf einem 32 Zoll großen 1080p-Bildschirm sieht hingegen verpixelt aus, weil der PPI-Wert unter 70 liegt.

Der PPI-Wert gehört zu den Dingen, die ein MacBook Pro so beeindruckend aussehen lassen. Der 15,4 Zoll große Bildschirm hat eine Auflösung von 2.880 x 1.800 Pixeln, was einem PPI-Wert von 220 entspricht. Schick! Moderne Smartphones besitzen enorme PPI-Werte – das ist der Grund dafür, dass die Darstellung so viel besser aussieht als auf einem typischen PC-Bildschirm.

Helligkeit

Die Stärke der Hintergrundbeleuchtung eines LCD-Bildschirms bestimmt die Helligkeit des Bildschirms. Die Helligkeit wird in *Nits* angegeben und liegt zwischen 100 und mehr als 1.000 Nits am oberen Ende. Durchschnittliche LCD-Bildschirme haben etwa 300 Nits, was größtenteils für eine ausgezeichnete Helligkeit gehalten wird.

Hinweis

Ein Nit entspricht einem Candela/m^2. Ein Candela wiederum entspricht in etwa der von einer Kerze ausgestrahlten Lichtmenge.

Blickwinkelabhängigkeit

LCD-Bildschirme weisen eine gewisse *Blickwinkelabhängigkeit* auf. Das bedeutet, dass die Darstellung verblasst, wenn man den Bildschirm von der Seite betrachtet (oder in einem Winkel, der nicht genau auf die Bildschirmmitte ausgerichtet ist). Bei TN-Bildschirmen ist der Blickwinkel, in dem das Bild noch gut aussieht, mit ca. 70 Grad relativ eng. Die Hersteller und Kunden sind nicht nur wegen der tollen Farben zur IPS-Technologie gewechselt, sondern auch wegen des im Vergleich mit TN-Bildschirmen deutlich größeren Blickwinkels (Abbildung 17.16). Achten Sie darauf, wenn Sie einen Monitor kaufen. Ein größerer Blickwinkel ist für typische Anwender besser. Ein enger Blickwinkel ist geeignet, wenn Sie verhindern möchten, dass irgendjemand außer dem eigentlichen Benutzer sehen kann, was auf dem Bildschirm dargestellt wird.

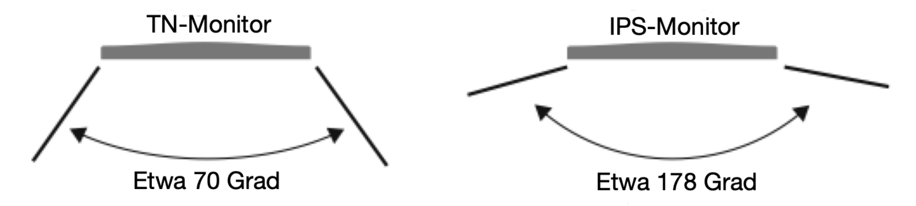


Abb. 17.16: Blickwinkelabhängigkeit

Tipp: Blickwinkelabhängigkeit von LCD-Bildschirmen testen

Besuchen Sie ein örtliches Computergeschäft, um LCD-Displays selbst in Augenschein zu nehmen. Und lassen Sie sich nicht von all den neuen Grafikkarten, Soundkarten, CPUs und Mainboards ablenken. Nun gut, ist schon in Ordnung, sich das anzusehen – vergessen Sie darüber aber nicht die Bildschirme!

Betrachten Sie den Bildschirm aus einer Entfernung von ca. 50 bis 60 cm. Blicken Sie direkt auf den Bildschirm und beurteilen Sie Bildqualität, Helligkeit und Farbintensität. Bewegen Sie sich nun ein wenig nach links oder rechts und vergleichen Sie die Qualität mit der vorherigen. Bewegen Sie sich allmählich weiter in die gewählte Richtung, bis Sie das Bild nicht mehr erkennen können. Sie haben nun die Grenze des Blickwinkels des Bildschirms überschritten.

Führen Sie diesen Test mit verschiedenen Bildschirmen durch. Ist der Blickwinkel bei kleineren Monitoren, wie etwa 20-Zoll-Geräten, geringer? Ist er bei großen Bildschirmen größer? Sie könnten auch die vertikale Blickwinkelabhängigkeit überprüfen. Blicken Sie auf einen Monitor, der sich auf Augenhöhe befindet, und betrachten Sie ihn dann von oben bzw. von unten. Gibt es eine vertikale Blickwinkelabhängigkeit? Es gibt inzwischen auch gekrümmte Bildschirme, die ich hier nicht erörtert habe. Welche Blickwinkelabhängigkeit weisen solche Geräte auf?

Reaktionszeit

Bei der Reaktionszeit eines LCD-Bildschirms handelt es sich um die Zeit, die es dauert, bis alle Subpixel von einem Zustand in einen anderen wechseln. Die Hersteller messen die LCD-Reaktionszeiten in Millisekunden – je niedriger, desto besser. Hierbei gibt es zwei Messmethoden. Zum einen, wie lange es dauert, bis alle Pixel von reinem Schwarz zu reinem Weiß und wieder zurück wechseln (*Black-to-White*, BtW), zum anderen, wie lange die Pixel benötigen, um von einem Grauwert zu einem anderen zu wechseln (*Gray-to-Gray*, GtG).

Der GtG-Wert ist immer niedriger als der BtW-Wert. Ein typisches modernes LCD-Display hat eine nominale Reaktionszeit von rund 5 ms. Die Hersteller geben fast immer nur den GtG-Wert an, ich habe aber ein LG-Display gefunden, bei dem beide Werte angegeben sind: 5 ms für GtG und 14 ms für BtW. Ältere Displays besitzen manchmal eine BtW-Reaktionszeit von mehr als 20 ms. Das ist so langsam, dass man beim Betrachten von Filmen oder schnellen Spielen Geisterbilder wahrnimmt.

Bildwiederholrate

Beim LCD-Monitor gibt die Bildwiederholrate an, wie oft der Bildschirminhalt geändert bzw. komplett neu aufgebaut werden kann. Wenn Sie sich die Bildwiederholrate bei einem LCD-Monitor als Metronom oder Taktgeber vorstellen, dann kommt dies der Funktionsweise näher. Bei den meisten Rechneranwendungen sind die 60 Hz in Ordnung, die sich als Industriestandard etabliert haben. Menschen nehmen Bilder, die sich mehr als etwa 24 Mal pro Sekunde ändern, als Bewegung wahr, nicht als eine Reihe einzelner Bilder. Dieser Wert wird auch bei Kinofilmen standardmäßig verwendet. Wenn der Bildschirm also fast drei Mal schneller aufgebaut werden kann, dann ist das selbst für Spiele mit schnellen Bewegungen mehr als ausreichend. Hochwertige Bildschirme übertreffen das aber noch und bieten Bildwiederholraten von 144, 165 oder 244 Hz.

Hinweis

Hochwertige Grafikkarten gehen weit über die Werte selbst der besten Bildwiederholraten hinaus. Siehe Abschnitt 17.5.3, *Adaptive Sync*, weiter hinten in diesem Kapitel.

Kontrastverhältnis

In so mancher Grafikabteilung gab es noch lange Röhrenmonitore, weil die ersten LCD-Bildschirme den Nachteil hatten, dass sie (insbesondere in heller Umgebung) nicht annähernd die Farbsättigung oder den Kontrast guter Bildröhren boten. Es war bis vor ein paar Jahren nichts Ungewöhnliches, in Designagenturen noch den einen oder anderen Röhrenmonitor vorzufinden.

Die LCD-Technologie wurde jedoch kontinuierlich verbessert und kann der Bildröhre inzwischen auch hier das Wasser reichen. Ein gutes Kontrastverhältnis (der Unterschied zwischen den dunkelsten und hellsten Farbtönen, die ein Bildschirm darstellen kann) liegt bei 450:1, ein kurzer Besuch im

Computerladen zeigt jedoch, dass es LCDs mit schlechteren (250:1), aber auch besseren Werten (1000:1) gibt.

LCD-Hersteller werben mit Angaben für das *dynamische Kontrastverhältnis* ihrer Bildschirme, bei dem der Unterschied zwischen einem voll erleuchteten, weißen Bildschirm und einem voll abgeschalteten, schwarzen Bildschirm gemessen wird. Dabei ergibt sich ein viel höherer Wert als bei dem ansonsten üblichen Kontrastverhältnis. Meine Samsung-Bildschirme haben z.B. ein Kontrastverhältnis von 1.000:1, aber ein dynamisches Kontrastverhältnis von 20.000:1. Klingt beeindruckend, oder? Allgemein hat das dynamische Kontrastverhältnis auf die Arbeit am Computermonitor keine Auswirkungen. Das dynamische Kontrastverhältnis hat im Allgemeinen bei Computerbildschirmen keine Auswirkungen auf die Darstellung. Konzentrieren Sie sich bei Ihrem Urteil über LCD-Bildschirme auf das Standard-Kontrastverhältnis.

Farbtiefe

Die Anzahl der Farben, die ein LCD-Bildschirm darstellen kann, wird als *Farbtiefe* bezeichnet. Sie spiegelt sich in der Bittiefe des LCD-Panels wider. Sehr alte TN-Monitore verwendeten beispielsweise ein 6-Bit-Panel. Das bedeutete, dass jeder Farbkanal – Rot, Grün und Blau – 64 (2^6) verschiedene Farben darstellen konnte. Die meisten heutigen Monitore verwenden 8-Bit-Panels, mit 256 (2^8) Farben pro Kanal. Im Marketing wird das als 24-Bit-Farbe bezeichnet und es bedeutet, dass ein Monitor 16,7 Millionen Farben darstellen kann. In hochwertigen Displays setzen die Hersteller 10-Bit-Panels ein, die 1.024 (2^{10}) Farben pro Kanal anzeigen und somit mehr als eine Milliarde Farben bieten. Dieser Anstieg der Anzahl der Farben wird sehr deutlich, wenn man häufig Fotos bearbeitet oder Farbkorrekturen an Videos vornimmt.

Vergleich von LCD-Bildschirmen

Es gibt also einiges zu beachten, wenn Sie für sich selbst oder für einen Kunden einen LCD-Bildschirm kaufen. Am wichtigsten dürften Größe und native Auflösung sein. Die Art der Technologie (TN, IPS oder VA) und die Hintergrundbeleuchtung (Randhintergrundbeleuchtung oder vollflächige Beleuchtung) haben Auswirkungen sowohl auf die Qualität als auch den Preis des Geräts. Da der Bildschirm das wichtigste Ausgabegerät des Computers ist und zu den langlebigsten Komponenten zählt, ist die Entscheidung für ein bestimmtes Modell von großer Tragweite.

Merken Sie sich für die Prüfung die Kriterien Auflösung, Helligkeit, Reaktionszeit und Farbtiefe. Heutzutage bieten die meisten Monitore hier akzeptable Werte.

Die große Mehrheit wird sich für ein IPS-Panel mit Randhintergrundbeleuchtung entscheiden. Die Anzahl der Farben und der Blickwinkel sind erstaunlich. Größe und Auflösung werden sowohl von Ihrem Budget als auch von der verfügbaren Stellfläche bestimmt. TN-Monitore besetzen zwei Nischen im Angebotsspektrum. Sie sind am preiswertesten, werden aber auch zum Spielen verwendet, denn keine andere Technologie kann TN-Monitoren bei der Reaktionszeit das Wasser reichen. TN-Monitore zum Spielen gehören jedoch auch zu den teuersten Displays, die angeboten werden. Somit sind TN-Bildschirme an beiden Enden des Preisspektrums zu finden.

17.1.3 Projektoren

Projektoren oder *Beamer* erzeugen ein Bild, das sie auf eine Leinwand (oder ein anderes Objekt) projizieren. Zu diesem Zweck müssen sie im richtigen Abstand vor der Leinwand platziert werden. Projektoren, die mit PCs verbunden sind, auf denen Microsoft PowerPoint läuft, sind seit den Zeiten der Clinton-Regierung in praktisch jedem Meeting zu finden (Abbildung 17.17). In diesem Abschnitt geht ausschließlich um diese Art von Projektoren.



Abb. 17.17: Ein Projektor (Foto mit freundlicher Genehmigung von Dell Inc.)

Projektortechnologien

Die erste Projektorgeneration verwendete Kathodenstrahlröhren. Jede Farbe verwendete eine separate Röhre, die das Bild auf einen Bildschirm projizierte (Abbildung 17.18). Röhrenprojektoren erzeugten wunderbare Bilder, waren aber teuer, groß und außerordentlich schwer und wurden mittlerweile fast vollständig von moderneren Technologien abgelöst.



Abb. 17.18: Röhrenprojektor

Angesichts der Tatsache, dass LCD-Panels lichtdurchlässig sind, eignen sich LCD-Projektoren optimal als Beamer. LCD-Projektoren sind leicht und viel preiswerter als Röhrenprojektoren, bieten aber nicht dieselbe Bildqualität (Abbildung 17.19).



Abb. 17.19: LCD-Projektor (Foto mit freundlicher Genehmigung von ViewSonic)

Die proprietäre DLP-Technologie (*Digital Light Processing*) von Texas Instruments verwendet eine rechteckige Anordnung winziger Spiegel, die durch einen Prozessor angesteuert werden, um ein Bild zu projizieren. Diese Technologie unterscheidet sich deutlich von LCDs. DLP-Projektoren liefern »wärmere« Bilder als LCD-Projektoren, aber das muss nicht unbedingt von Nachteil sein, insbesondere bei hochauflösenden Inhalten wie Spielfilmen. DLP-Projektoren benötigen mehr Energie, sind aber nicht so schwer wie LCD-Projektoren. Treffen Sie Ihre Auswahl mit Bedacht!

Alle Projektoren besitzen prinzipiell dieselben Eigenschaften wie Bildschirme, die mit der gleichen Technologie arbeiten. So haben beispielsweise LCD-Projektoren alle eine natürliche, feste Auflösung. Sie sollten drei für Projektoren spezifische Begriffe kennen: Lumen, Projektionsdistanz und Lampen.

Lumen

Die Helligkeit von Projektoren wird in *Lumen* angegeben. Ein Lumen entspricht der Lichtmenge, die eine Lichtquelle festgelegter Helligkeit in einen bestimmten Raumwinkel abstrahlt und die das menschliche Auge wahrnimmt. Je größer der Lumenwert eines Projektors ist, desto heller ist er. Die jeweils besten Lumenwerte sind von der Raumgröße und von der dort vorhandenen Beleuchtung abhängig. Es gibt keine allgemeingültige Empfehlung für den »richtigen« Lumenwert eines Projektors, aber Richtwerte: Wenn Sie einen Projektor in einem kleinen, abgedunkelten Raum verwenden, sind 1.000 bis 1.500 Lumen völlig ausreichend. Wenn Sie dagegen einen Projektor in einem mittelgroßen Raum mit typischer Beleuchtung einsetzen, benötigen Sie mindestens 2.000 Lumen. Projektoren für große Räume kommen sogar auf Werte von 10.000 Lumen und sind sehr teuer.

Projektionsdistanz

Die *Projektionsdistanz* ist ein Maß für die Größe des Bildes bei einem bestimmten Abstand der Leinwand. Alle Projektoren haben eine empfohlene minimale und maximale Projektionsdistanz, die Sie berücksichtigen sollten. Eine typische Projektionsdistanz kann als der Abstand ausgedrückt werden, der erforderlich ist, um eine Bildschirmdiagonale von 2,5 Metern zu erhalten. Ein normaler Projektor muss etwa 3,5 Meter von der Leinwand entfernt sein. Ein Projektor mit einer *Short-Throw-Linse* kann diesen Abstand auf etwa 1,2 Meter verringern. Verfügt der Projektor über eine Ultra-Short-Throw-Linse, genügt ein Abstand von nur rund 40 Zentimetern, diese Linsen sind allerdings sehr kostspielig. In Abbildung 17.20 sind verschiedene Projektionsdistanzen dargestellt.

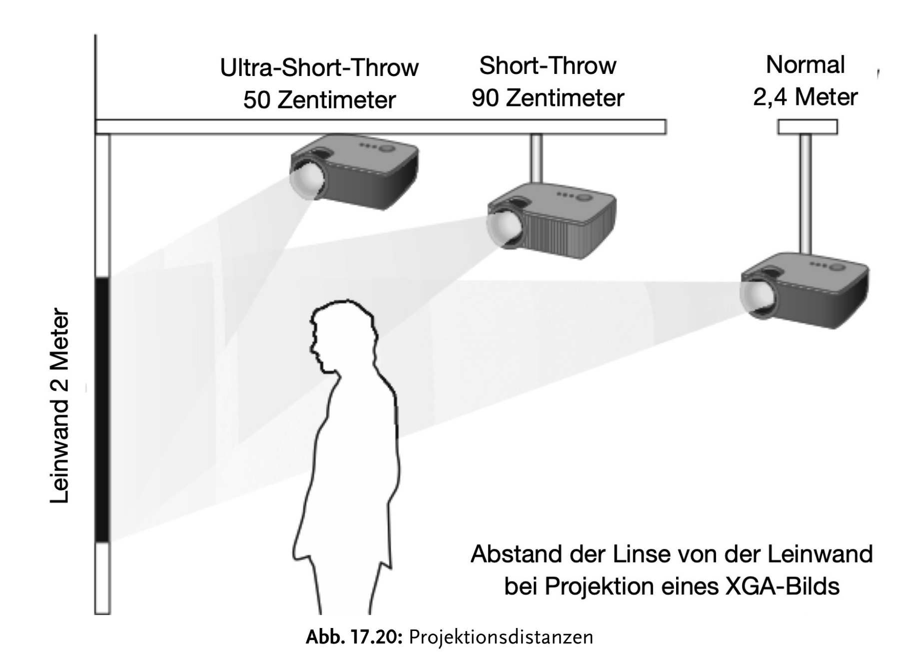


Abb. 17.20: Projektionsdistanzen

Lampen

Lampen sind die Schwachstelle aller Projektoren. Lampen leisten Schwerstarbeit im Projektor, weil sie eine enorme Menge an Licht produzieren müssen. Daher erzeugen sie relativ viel Wärme, und alle Projektoren benötigen Lüfter, die ein Überhitzen der Lampen verhindern. Wenn Sie einen Projektor ausschalten, läuft der Lüfter weiter, bis die Lampe vollständig abgekühlt ist. Lampen sind sehr teuer und kosten oft mehrere Hundert Euro, was für so manchen Benutzer, der beim Ausfall der Lampe nicht auf derartige Preise gefasst ist, einen veritablen Schock darstellt!

Die meisten Projektoren verwenden Halogen-Metalldampflampen, LEDs oder Laser. Halogen-Metalldampflampen waren jahrelang der Standard. Diese Lampen erzeugen auf kleinstem Raum eine enorme Anzahl von Lumen. Die Nachteile: Sie werden sehr heiß, was mit einem ständigen Lüftergeräusch verbunden ist, die durchschnittliche Lebensdauer beträgt nur etwa 3.000 Stunden und sie sind sehr teuer.

LED-Projektoren verwenden zum Erzeugen von Licht rote, grüne und blaue LEDs. LEDs werden nicht heiß, deshalb können kleinere und leisere Lüfter verwendet werden. LED-Projektoren waren lange erheblich teurer als Projektoren mit Halogen-Metalldampflampen, aber der Preisunterschied hat sich deutlich verringert. Sie können allerdings bei Weitem nicht so viele Lumen erzeugen und machen daher dunklere Räume erforderlich. Andererseits haben LED-Lampen eine Lebensdauer von mehr als 20.000 Stunden.

Es gibt verschiedene Typen von Projektoren, die Laser verwenden. Manche nutzen weißes Laserlicht, das auf farbige Scheiben gelenkt wird, andere besitzen farbige Laser. Laser-Projektoren liefern leuchtende, kontrastreiche Bilder und erzeugen nur wenig Wärme. Die Lampen haben eine Lebensdauer von mehr als 30.000 Stunden. Die Geräte sind derzeit noch teurer als die konkurrierenden Technologien, die Preise sinken allerdings.

17.1.4 VR-Headsets

VR-Headsets sollen ein intensives und umfassendes Erleben der virtuellen Realität (VR) ermöglichen, indem zwei hochauflösende kleine Bildschirme in einem Headset montiert werden, das externe visuelle Störung abschirmt (Abbildung 17.21). Sie ermöglichen es dem Träger, eine 360 Grad umfassende Welt zu betreten, sodass es sich anfühlt, als befände man sich an einem anderen Ort und in einer anderen Zeit. Es gibt noch nicht viele Haushalte oder Organisationen, die VR verwenden, aber die modernen VR-Headsets gewähren schon einen Einblick in eine mögliche zukünftige Entwicklung der Computertechnologie.



Abb. 17.21: Innenansicht eines Headsets Vive Pro von HTC

Mithilfe eines sehr leistungsstarken Systems kann VR einen Betrachter in eine völlig andere Welt versetzen. Mit Google Earth VR ist es beispielsweise möglich, vom heimischen Sofa aus durch die Straßen von Paris zu wandern, den Mount Everest zu ersteigen, während man am Strand in der Sonne liegt, oder mit den Astronauten der Internationalen Raumstation abzuhängen, ohne den Planeten Erde zu verlassen. Und das ist nur die Spitze des Eisbergs.

Noch ist VR vor allem etwas für Enthusiasten, aber die Technologie hat in den letzten Jahren große Fortschritte gemacht, insbesondere durch die Verbesserung der winzigen Displays. Aktuelle VR-Headsets verwenden die OLED-Technologie (*Organic Light-Emitting Diode*) oder Aktiv-Matrix-OLEDs (AMOLED) mit zusätzlichen Transistoren für die hochauflösenden Stereo-Panels.

OLEDs unterscheiden sich von LEDs in mehrfacher Hinsicht. OLEDs verwenden zwischen den Glasschichten organische Verbindungen, die aufleuchten, wenn ihnen elektrische Ladungen zugeführt werden. Das bedeutet, dass sie keine Hintergrundbeleuchtung benötigen. Deshalb sind sie perfekt für extrem dünne und energiesparende Displays geeignet. Und weil es keine Hintergrundbeleuchtung gibt, können OLED-Pixel komplett ausgeschaltet werden, was ein reines Schwarz ermöglicht und im Vergleich mit LCD-Panels einen phänomenalen Kontrast bietet.

OLED hat sich bislang in drei Nischen etablieren können: in hochwertigen Fernsehern, in kleinen mobilen Geräten (wie Smartwatches oder Smartphones) und in VR-Headsets.

Hinweis

Lesen Sie die Erläuterungen über MicroLED im Abschnitt *Jenseits von A+*, um mehr über einen potenziellen Konkurrenten für OLED und LCD zu erfahren. In Kapitel 24, *Mobile Geräte*, werde ich ebenfalls auf OLED zurückkommen.

17.1.5 Gemeinsame Merkmale

Alle Monitore besitzen eine Reihe von Merkmalen, die Sie für den Einkauf, die Installation, die Wartung und die Fehlersuche kennen müssen. Sie unterscheiden sich durch verschiedene Steckertypen, Einstellungsmöglichkeiten auf dem Bildschirm, Halterungen und zusätzliche Features, wie eingebaute USB-Hubs, Webcams, Lautsprecher und Mikrofone.

Anschlüsse

Monitore werden mit einem der folgenden sechs Anschlüsse mit dem Computer verbunden:

- VGA
- DVI
- HDMI
- DisplayPort
- Thunderbolt
- HDBaseT

VGA Viele PC-Monitore verwenden den bekannten 15-poligen, dreireihigen *DB-Anschluss* (Abbildung 17.22), der oft auch *D-Sub-Anschluss* oder meistens *VGA-Anschluss* genannt wird. VGA ist der älteste und leistungsschwächste Monitoranschluss.

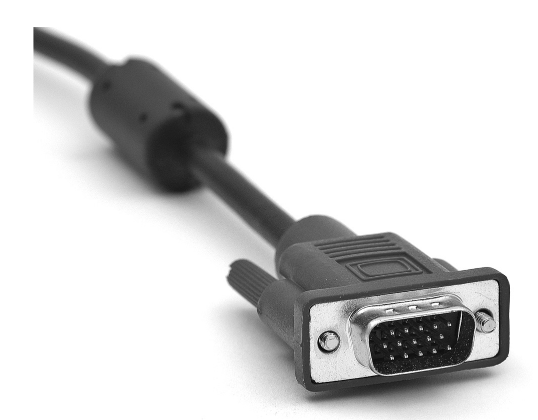


Abb. 17.22: VGA-Anschluss

DVI Viele LCD-Bildschirme verwenden den *DVI*-Standard (*Digital Visual Interface*). Bei DVI handelt es sich eigentlich um drei verschiedene Anschlüsse, die sich sehr ähnlich sind. *DVI-D* dient dem digitalen und *DVI-A* dem analogen Anschluss (wenn der Monitorhersteller die Abwärtskompatibilität wünscht). Mit *DVI-A/D* oder *DVI-I* (*Interchangeable*) lassen sich schließlich sowohl DVI-D- als auch DVI-A-Stecker verbinden. DVI-D und DVI-A sind so codiert, dass sie sich nicht versehentlich falsch anschließen lassen.

DVI-D- und DVI-I-Anschlüsse gibt es in zwei Varianten, mit einfacher Verbindung (*Single Link*) und doppelter Verbindung (*Dual Link*). Single-Link-DVI hat eine maximale Bandbreite von 165 MHz, was in der Praxis die maximale Auflösung eines Bildschirms auf 1.920 x 1.080 bei 60 Hz oder 1.280 x 1.024 bei 85 Hz beschränkt. Dual-Link-DVI verwendet mehr Pins, um den Durchsatz zu verdoppeln, und erlaubt deshalb höhere Auflösungen (Abbildung 17.23). Mit Dual-Link-DVI können Sie Bildschirme mit Auflösungen von bis zu 2.048 x 1.536 bei 60 Hz betreiben.

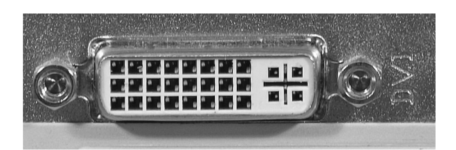


Abb. 17.23: Dual-Link-DVI-I-Anschluss

HDMI Viele LCDs, Projektoren und VR-Headsets werden per HDMI-Anschluss mit dem Computer verbunden, der sowohl hochauflösende Videosignale als auch Audiodaten liefert (Abbildung 17.24). HDMI kann problemlos so ziemlich jede Auflösung eines Monitors ansteuern. HDMI ermöglicht es beispielsweise, Laptops an hochwertige Projektoren anzuschließen und brillante Multimediapräsentationen zu erzeugen. Viele kleinere Geräte verfügen über einen Mini-HDMI-Anschluss. Deshalb muss ein Kabel verwendet werden, das an einem Ende einen Mini-HDMI-Anschluss und am anderen Ende einen normalen HDMI-Anschluss besitzt. Aber das funktioniert tadellos!

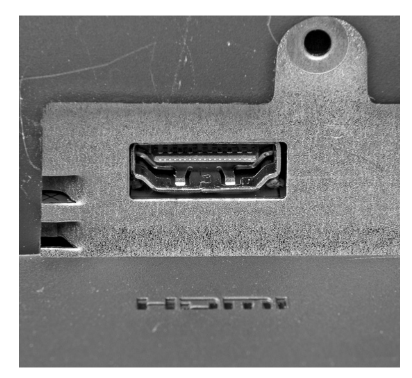


Abb. 17.24: HDMI-Buchse eines Monitors

DisplayPort und Thunderbolt Manche Monitore werden entweder über *DisplayPort* (DP) oder *Thunderbolt* mit dem Computer verbunden. Beide unterstützen hochauflösende Grafik und Audio.

Dass ich die beiden Anschlüsse hier zusammen nenne, hat einen Grund. DP-Anschlüsse normaler Größe sind heute üblich, wie bei meinem Dell-Monitor (Abbildung 17.25). Daran werden DP-Stecker normaler Größe angeschlossen, wie man es erwarten würde.

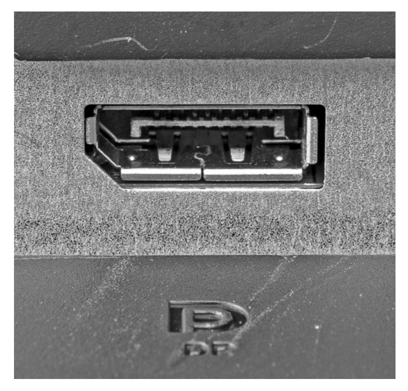


Abb. 17.25: DisplayPort-Anschluss eines Monitors

Thunderbolt 1 und Thunderbolt 2, die Sie aus Kapitel 10 kennen, verwenden den gleichen Anschluss wie die kleine Variante von DisplayPort, die *Mini-DisplayPort* (mDP) heißt. Thunderbolt 3 wiederum verwendet Stecker des Typs USB-C. Deshalb eine Warnung: Es gibt Monitore, die über ein mDP-mDP-Kabel angeschlossen werden, ohne Thunderbolt 1 oder 2 zu verwenden, und viele UCB-C-Stecker und -Kabel unterstützen Thunderbolt 3 nicht. Halten Sie nach den kleinen Symbolen neben dem Anschluss Ausschau, um festzustellen, welche Technologie bei der Verbindung von Computer und Bildschirm zum Einsatz kommen sollte (Abbildung 17.26).

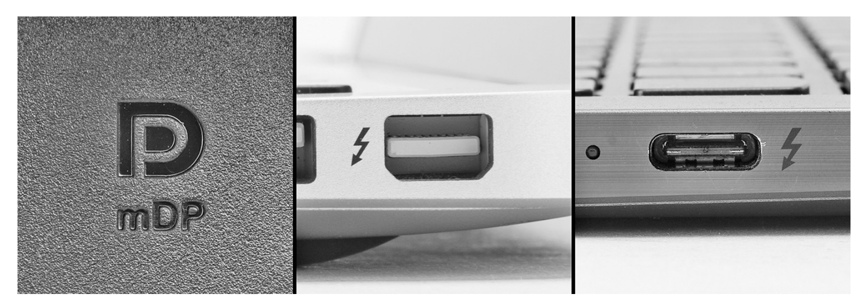


Abb. 17.26: Einfacher mDP-Anschluss (links), Thunderbolt 2 mDP (Mitte) und Thunderbolt 3 USB-C (rechts)

HDBaseT Einige Projektoren verwenden eine Verbindungstechnologie namens *HDBaseT*, die es ermöglicht, unkomprimierte hochauflösende Videos und Audio über größere Distanzen mit Netzwerkkabeln der Kategorie 5a oder 6 zu übertragen (Abbildung 17.27). Ich habe Netzwerkkabel noch nicht erörtert (dazu komme ichin Kapitel 19), aber merken Sie sich diese Technologie. Sie bedeutet in der Praxis, dass Sie Projektoren in Konferenzräumen über Kabel anschließen können, die bis zu 100 Meter lang sein dürfen. Wenn der Projektor HDBaseT nicht direkt unterstützt, können Sie einen HSBaseT-Empfänger verwenden, der die Signale in etwas konvertiert, das der Projektor nutzen kann. HDBaseT ist kein Bestandteil der Zertifizierungsprüfung, aber Sie können der Technologie in der Praxis durchaus begegnen.



Abb. 17.27: HDBaseT-Anschluss eines Projektors

Adapter Früher oder später werden Sie in die Situation geraten, dass ein Monitor einen anderen Videoanschluss besitzt als der Computer. In der Zertifizierungsprüfung wird davon ausgegangen, dass Sie einen kleinen Adapter verwenden, wie den DVI-VGA-Adapter in Abbildung 17.28. Ebenfalls gebräuchlich sind DVI-HDMI-Adapter. Apple und andere Hersteller haben in ihre besonders dünnen Laptops Thunderbolt-Anschlüsse integriert. Die Adapterhersteller bieten daher auch Thunderbolt-DVI- und Thunderbolt-HDMI-Adapter an.



Abb. 17.28: DVI-VGA-Adapter

Alternativ können Sie auch Kabel verwenden, die an beiden Enden verschiedene Anschlüsse besitzen. Abbildung 17.29 zeigt ein typisches DVI-HDMI-Kabel. Viele neue Geräte verfügen nur noch über USB-C-Anschlüsse zur Ausgabe (etwa einfache USB-C-Anschlüsse oder Thunderbolt-fähige USB-C-Anschlüsse). Wenn der Bildschirm keinen passenden Anschluss besitzt, müssen Sie womöglich ein USB-C-mDP- oder ein USB-C-HDMI-Kabel verwenden, um eine Verbindung herzustellen.



Abb. 17.29: DVI-HDMI-Kabel

Einstellungen

Die meisten Monitoreinstellungen werden im Rahmen der Installation vorgenommen. Hier geht es erst einmal nur darum zu wissen, was sich einstellen lässt und wo sich diese Einstellungen vornehmen lassen. Natürlich besitzen alle Monitore einen Netzschalter. Üblicherweise gibt es auch Helligkeits- und Kontrastregler. Darüber hinaus verfügen die meisten Monitore (zumindest jene, zu deren Kauf sich raten lässt) über ein integriertes Menüsystem, über das man eine Reihe von Einstellungen vorneh-

men kann. Der Zugang zu diesen Menüs ist bei den verschiedenen Herstellern unterschiedlich geregelt, sie weisen aber durchweg zwei Hauptfunktionen auf, zu denen die Größe der Darstellung (größer, kleiner, nach links, rechts, oben und unten verschieben usw.) und die Farbanpassung zählen. Im Rahmen der Farbanpassung lassen sich die Farbintensitäten (rot, grün, blau) so einstellen, dass man möglichst naturgetreue Farbtöne erhält. All diese Einstellungen werden von persönlichen Vorlieben beeinflusst. Sorgen Sie dafür, dass der jeweilige Anwender des Rechners weiß, wie er diese Einstellungen ändern kann (Abbildung 17.30).



Abb. 17.30: Typische Menüsteuerung für die Monitoreinstellungen

VESA-Halterungen

Fast alle Monitore verfügen über eine standardisierte Befestigungsmöglichkeit, um ein Gerät beispielsweise an der Wand zu montieren oder an einem Ständer festzuschrauben, die als VESA-Halterung bezeichnet wird (Abbildung 17.31). In Abbildung 17.32 ist ein Monitorständer zu sehen, an dem zwei Bildschirme mit VESA-Halterungen befestigt werden können. Die genaue Form der VESA-Halterungen hängt von den Geräten ab, ein großer Fernseher verwendet also eine größere Halterung als ein typischer 24-Zoll-Monitor.



Abb. 17.31: VESA-Halterung eines Monitors



Abb. 17.32: Monitorständer mit zwei VESA-Halterungen

Hinweis

Für die verschiedenen standardisierten VESA-Halterungen gibt es eine Reihe von offiziellen Bezeichnungen. Sie finden sie in der Literatur unter den Bezeichnungen FDMI (*Flat Display Mounting Interface*) und MSI (*Mounting Interface Standard*). Für gekrümmte Bildschirme gibt es keine VESA-Halterungen.

Zusätzliche Features

Einige Monitorhersteller fügen ihren Produkten zusätzliche Features hinzu, beispielsweise USB-Hubs, Lautsprecher, Webcams und Mikrofone. Für Techniker ist das an einem USB-Anschluss des Typs B am Monitor erkennbar, der mit einem USB-Anschluss des Typs A am Rechner verbunden wird, so wie andere Peripheriegeräte auch. Wenn Sie heutzutage einen Monitor kaufen, verfügt er möglicherweise über einen USB-C-Anschluss, der mit einem USB-C-Anschluss des Computers verbunden wird. Der Standard wird sich vermutlich in naher Zukunft ändern (oder hat sich schon geändert, wenn Sie diese Zeilen lesen). Abbildung 17.33 zeigt die USB-Anschlüsse an der Seite eines Bildschirms – das ist wirklich äußerst praktisch!



Abb. 17.33: USB-Anschlüsse eines Monitors

17.2 Grafikkarten

Die Grafikkarte verarbeitet im PC die Daten des Prozessors, bereitet sie auf und überträgt diese zum Bildschirm. Grafikkarten sind ziemliche komplexe Geräte. Ein Grafikprozessor bestimmten Typs nimmt Daten von der CPU entgegen und leitet Befehle an den Bildschirm weiter. Wie jeder andere Prozessor auch benötigt er RAM. Außerdem ist eine schnelle Verbindung zwischen Grafikprozessor, CPU und System-RAM erforderlich. Dass die Grafikkarte einen zum Bildschirm passenden Anschluss besitzen muss, versteht sich von selbst.

Üblicherweise handelt es sich bei einer Grafikkarte um eine Erweiterungskarte, die auf dem Mainboard eingebaut wird (Abbildung 17.34). Obwohl heute bei vielen neuen Systemen die Schaltkreise der Grafikkarte Teil des Mainboards sind, sprechen die meisten Techniker weiterhin von der Grafikkarte. Dieser Abschnitt befasst sich mit den fünf Aspekten, die eine Grafikkarte ausmachen: Mainboard-Steckplatz, Grafikprozessor, Video-RAM, integrierte GPUs und Anschlüsse.

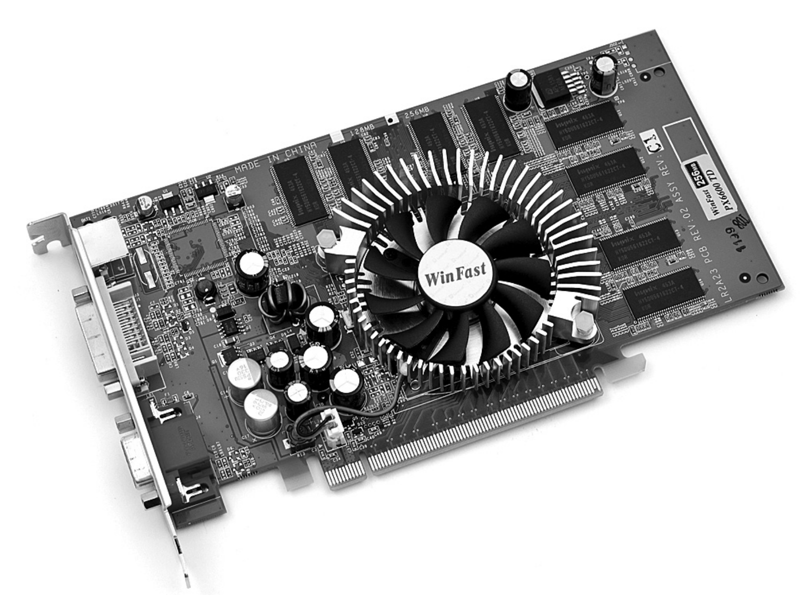


Abb. 17.34: Typische Grafikkarte

17.2.1 Mainboard-Anbindung

Als Techniker werden Ihnen vier verschiedene Anschlussmöglichkeiten begegnen, die bei der Mainboard-Anbindung verwendet werden. Die älteste Anschlussart ist PCI, das heute nur noch für zusätzliche Grafikkarten zum Anschluss weiterer Monitore an ältere Systeme genutzt wird. Etwas jünger, aber ebenfalls schon ziemlich alt ist AGP. Alle aktuellen Grafikkarten sind für den PCIe-Anschluss ausgelegt. Und schließlich gibt es viele Mainboards mit eingebauter Grafikkarte. Die integrierten Grafikkarten werde ich erläutern, nachdem Grafikprozessoren und Speichertypen vorgestellt sind, da dies dem Zusammenhang nach sinnvoller ist. Zunächst betrachten wir PCI, AGP und PCIe.

PCI

Die Nutzung höherer Farbtiefen verlangsamt die Bildschirmausgabe. Die von der Grafikkarte zum Bildschirm transportierten Daten müssen über die Speicherchips der Grafikkarte und den Erweiterungsbus übertragen werden, deren Geschwindigkeit begrenzt ist. Die in fast allen Systemen vorhandenen Standard-PCI-Steckplätze sind auf 32-Bit-Transfers bei etwa 33 MHz beschränkt, woraus sich

eine maximale Bandbreite von 132 MBps ergibt. Das scheint zwar viel zu sein, relativiert sich bei Nutzung höherer Auflösungen, Farbtiefen und Bildwiederholraten aber schnell. (Die Bildwiederholrate war von Bedeutung, denn zu PCI-Zeiten gab es nur Röhrenmonitore.) Darüber hinaus verwendeten fast alle Systeme mehrere PCI-Geräte, für die Bandbreite erforderlich war. Der PCI-Bus ist für die Ansprüche, die heutzutage an die Grafik gestellt werden, einfach zu langsam.

AGP

Mit *AGP* (*Accelerated Graphics Port*) kam Intel dem Wunsch nach einer höheren Grafikbandbreite nach. Bei AGP handelt es sich um einen einzelnen, speziellen Anschluss, der einem PCI-Steckplatz zwar ähnelt, der aber speziell für Grafikkarten vorgesehen war. Es gab keine Mainboards mit zwei AGP-Steckplätzen; tatsächlich besitzen aktuelle Mainboards überhaupt keinen AGP-Steckplatz, sie finden ihn nur noch bei älteren Systemen. Abbildung 17.35 zeigt einen AGP-Steckplatz der ersten Generation.

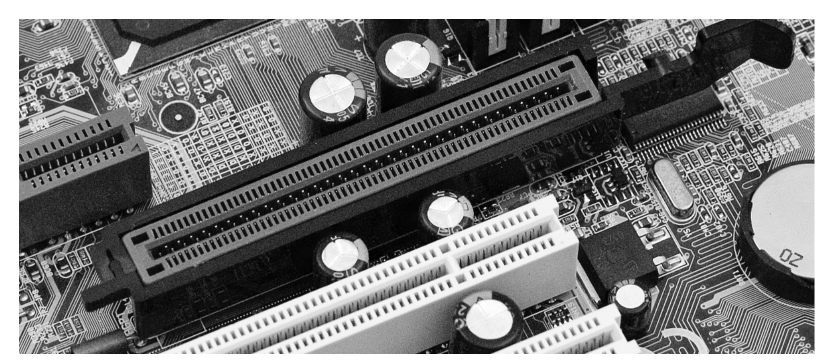


Abb. 17.35: AGP-Steckplatz

PCIe

Die PCI-Express-Schnittstelle (PCIe) wurde als designierter PCI-Nachfolger entwickelt und die Entwickler setzten alles daran, auch AGP abzulösen. PCIe ist eine natürliche Weiterentwicklung für Grafikkarten, weil es unglaublich schnell ist. Alle PCIe-Grafikkarten verwenden den PCIe-x16-Steckplatz (Abbildung 17.36). PCIe konnte AGP als primäre Grafikschnittstelle beinahe von einem Tag auf den anderen ersetzen.

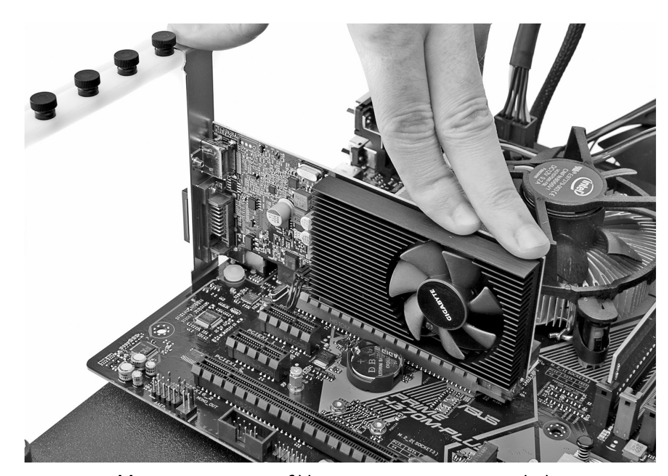


Abb. 17.36: PCIe-Grafikkarte in einem PCIe-Steckplatz

17.2.2 Grafikprozessoren

Der *Grafikprozessor* (*GPU – Graphics Processing Unit*) leistet die eigentliche Arbeit und übernimmt und übersetzt die Befehle von der CPU in vom Bildschirm verstandene Koordinaten und farbige Darstellungen.

In Gesprächen, die sich um Grafikkarten drehen, geht es (zumindest unter Technikern) fast immer um verwendete Grafikprozessoren und die Speicherkapazitäten der Karten. Eine typische Grafikkarte könnte z.B. MSI GeForce GTX 1080ti 11-GB 384-Bit GDDR5X PCI Express 3.0 heißen. Das wollen wir jetzt genauer betrachten. MSI heißt der Hersteller, GeForce GTX 1080ti ist der Grafikprozessor, 11-GB 384-Bit GDDR5 weist auf die Kapazität des Video-RAMs und die Verbindung zwischen Video-RAM und Grafikprozessor hin und PCI Express 3.0 schließlich beschreibt die Art des erforderlichen Erweiterungssteckplatzes auf dem Mainboard.

Hinweis

Viele Grafikkarten sind mit einer Kopierschutztechnologie namens HDCP (*High-bandwidth Digital Content Protection*) ausgerüstet. HDCP verhindert das Kopieren von Audio und Video über Anschlüsse mit hoher Bandbreite, wie HDMI, DisplayPort oder DVI. Zudem verhindert die Technologie auf entsprechend ausgestatteten Geräten die Wiedergabe von HDCP-geschützten Inhalten.

Es gibt zwar viele Unternehmen, die Hunderte verschiedener Grafikkarten anbieten, aber nur drei Unternehmen, die den Löwenanteil der aktuell auf Grafikkarten eingesetzten Grafikprozessoren herstellen: NVIDIA, AMD und Intel. NVIDIA und AMD stellen Grafikprozessoren her und verkaufen sie an Dritthersteller, die dann eigene Grafikkarten entwickeln, herstellen und unter ihrem eigenen Markennamen anbieten. Intel bot auch eine eigene Palette von Grafikkarten an, konzentriert sich aber nun auf in Mainboards integrierte Grafikprozessoren. Abbildung 17.37 zeigt eine NVIDIA GeForce GTX 570 auf einer Steckkarte der Firma EVGA.



Abb. 17.37: NVIDIA GeForce GTX 570

Die Auswahl des Grafikprozessors ist die wohl wichtigste Einzelentscheidung beim Kauf einer Grafikkarte. Preiswerte Grafikprozessoren eignen sich üblicherweise gut für den Durchschnittsanwender, der Briefe schreiben oder mit einem Webbrowser arbeiten will. High-End-Grafikprozessoren werden entwickelt, um die jeweils aktuell beliebten 3-D-Spiele zu unterstützen und um die Wiedergabe hochauflösender Videos zu ermöglichen. Einige 3-D-Aspekte kommen in diesem Kapitel noch zur Sprache.

17.2.3 Video-RAM

Der Grafikspeicher ist für den Betrieb des Rechners unverzichtbar. Bei ihm handelt es sich wahrscheinlich um jene elektronischen Bauteile, die im PC am härtesten arbeiten müssen. Video-RAM wird laufend aktualisiert und spiegelt alle Änderungen auf dem Bildschirm wider. Es gibt beim Grafikspeicher drei ernsthafte Engpässe, wenn Sie mit sehr leistungshungrigen Programmen (wie etwa Spielen) arbeiten: Datendurchsatzgeschwindigkeit, Zugriffsgeschwindigkeit und die Speicherkapazität an sich.

Die Hersteller haben diese Flaschenhälse dadurch überwunden, dass sie die Breite des Busses zwischen dem Video-RAM und dem Grafikprozessor vergrößert haben, indem sie spezielle, superschnelle RAM-Bausteine einsetzen und immer mehr Arbeitsspeicher hinzufügen.

Die Hersteller haben den Grafikspeicher auf den Karten von der typischen 32 Bit breiten Struktur auf 64, 128 oder sogar 256 Bit erweitert. Dies wäre kein großer Vorteil, da ja der Systembus weiterhin auf 32 bzw. 64 Bit beschränkt bleibt, wenn es sich bei den meisten Grafikkarten nicht eigentlich um Platinen mit grafischen Koprozessoren handeln würde. Das Rendering und die Verarbeitung werden größtenteils von dem Grafikprozessor auf der Grafikkarte selbst und nicht vom Systemprozessor übernommen. Das Hauptsystem liefert lediglich die Eingangsdaten für den Prozessor auf der Grafikkarte. Durch den Speicherbus auf der Grafikkarte, der sehr viel breiter als der Standard-64-Bit-Übertragungsweg ist, lassen sich Daten viel schneller manipulieren und zum Monitor übertragen (Abbildung 17.38).

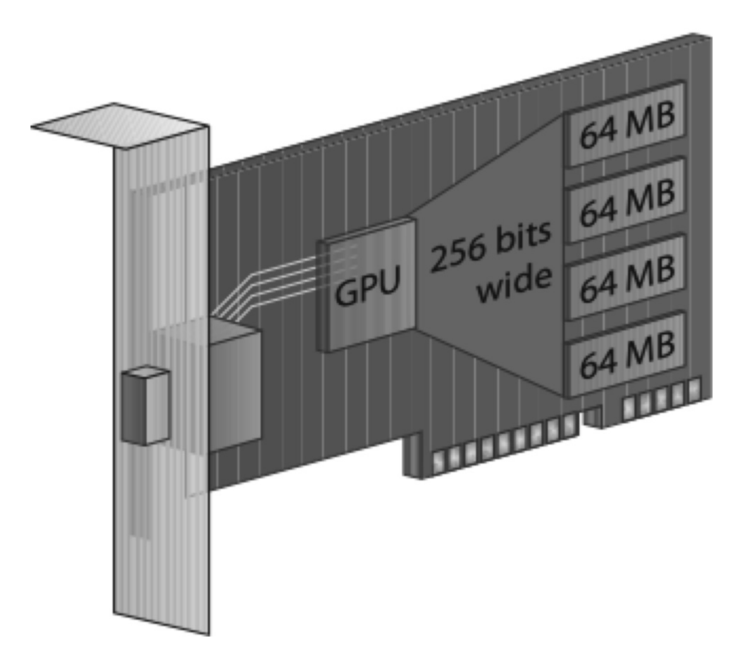


Abb. 17.38: Der breite Übertragungsweg zwischen Grafikprozessor und Video-RAM

Die Hersteller haben eine Reihe spezieller RAM-Varianten entwickelt, mit denen die Ausgabegeschwindigkeit deutlich steigt. Der wichtigste Unterschied zwischen DRAM und Video-RAM besteht darin, dass Grafik-RAM gleichzeitig Daten lesen und schreiben kann. Tabelle 17.1 führt einige der heute gebräuchlichen Video-RAM-Technologien auf, aber achten Sie darauf, dass Sie (gerade bei sehr preiswerten Modellen) auf Grafikkarten stoßen können, die irgendeine Version DDR-RAM verwenden.

Akronym	Name	Zweck
DDR3	Double Data Rate SDRAM Version 3	Wird für preiswerte Grafikkarten und Laptop-Grafikkarten verwendet
GDDR3	Graphics Double Data Rate Version 3	Wie DDR3, wird aber schneller getaktet; andere Kühlung erforderlich
GDDR4	Graphics Double Data Rate Version 4	Upgrade von GDDR3, höhere Taktung
GDDR5	Graphics Double Data Rate Version 5	Nachfolger von GDDR4; verdoppelt die E/A-Rate von GDDR4
GDDR5X	Graphics Double Data Rate Version 5X	Nachfolger von GDDR5
GDDR6	Graphics Double Data Rate Version 6	Nachfolger von GDDR5X
HBM	High Bandwidth Memory	Wettbewerber von DDR5
HBM2	High Bandwidth Memory Version 2	Nachfolger von HBM; Wettbewerber von GDDR6

Tabelle 17.1: Video-RAM-Technologien

Ein Großteil der Grafikkarten, insbesondere die zum Einsatz mit leistungshungrigen Spielen gedachten, verwenden GDDR5 oder GDDR5X. Bei einfacheren Grafikkarten am anderen Ende des Leistungsspektrums wird vor allem DDR3-RAM eingesetzt. HBM2 bietet im Vergleich zu DDR oder GDDR eine völlig andere Form von Speicher, bei der gestapelte DRAM-Chips über extrem breite Busse verbunden werden. GDDR2 verwendet eine Busbreite von 32 Bit, HBM hingegen 1.024 Bit. Der Wettbewerb der Speichertechnologien hat gerade erst angefangen und HBM und HBM2 kommen in der Zertifizierungsprüfung nicht vor, aber Sie sollten sie kennen.

Schließlich bieten viele fortgeschrittene 3-D-Grafikkarten hohe Video-RAM-Kapazitäten. Häufig findet man Karten mit 1, 2, 3 oder sogar 4 GB RAM! (Wenn Sie bereits sind, genügend Geld auf den Tisch zu legen, können Sie auch eine Grafikkarte mit bis zu 24 GB RAM bekommen.) Warum so viel? Selbst mit PCI Express dauert der Zugriff auf Daten im System-RAM immer deutlich länger als der Zugriff auf Daten im lokalen Arbeitsspeicher der Grafikkarte. Durch den riesigen Video-RAM-Speicher können Spielentwickler ihre Spiele optimieren und mehr wichtige Daten lokal im Video-RAM speichern.

17.2.4 Integrierte GPUs

Viele aktuelle Mainboards bringen eine integrierte GPU mit oder sind dafür vorbereitet, eine CPU mit integrierter GPU aufzunehmen. Die GPU des Mainboards ist entweder ein eigenständiger Chip oder Teil der Northbridge. Wenn ein Mainboard eine eigene GPU enthält, spricht man auch von Onboard-Grafik. Onboard-Grafik ist nicht besonders leistungsstark, in Laptops aber ziemlich verbreitet, denn sie ist platz- und energiesparend.

AMD und NVIDIA stellen integrierte GPU-Chips her, und Intel hat lange Zeit *GMA* (*Intel Graphics Media Accelerator*) in seine Chipsätze integriert. Einige der AMD-Prozessoren der Fusion-Serie können so mancher Kombination aus CPU und eigenständiger Grafikkarte das Wasser reichen (wenn auch nur im Bereich tragbarer Computer). Für ein gelegentliches Spiel und sogar halbwegs anspruchsvolle Spiele sind diese Prozessoren schon ausreichend. Intels GMA ist vollständig auf Bürocomputer ausgelegt und nicht für Spiele. NVIDIAs Tegra-Produktlinie hingegen ist für Spiele auf mobilen Geräten (wie Nintendo Switch) und Unterhaltungssysteme in Fahrzeugen gedacht.

Bei CPUs mit integrierter GPU wird es ziemlich eng auf dem Chip. Auf einem einzigen AMD-APU-Chip (*Accelerated Processing Unit*) drängen sich beispielsweise zwei bis vier Prozessorkerne, ein Speicher-Controller zur Unterstützung von DDR4, Cache-Speicher und ein Grafikprozessor, der erweiterte 3-D-Grafik beherrscht. Donnerwetter! Aber das Beste an dieser hochgradigen Integration ist, dass der Chip sehr viel weniger Energie benötigt als vergleichbare eigenständige Komponenten.

17.2.5 Anschlüsse und zugehörige Kabel

An den verschiedenen Grafikkarten finden sich eine Reihe verschiedener Anschlüsse, die teilweise sogar noch unterschiedliche Varianten aufweisen. Die CompTIA unterscheidet zwischen den Bezeichnungen der Anschlüsse der Karten und den dazugehörigen Kabeln, obwohl die meisten Techniker beide Bezeichnungen synonym verwenden. Die Details folgen.

Grafikkarten werden mit einem dieser sechs Anschlüsse mit einem Monitor verbunden:

- VGA
- DVI
- HDMI (inklusive der Mini- und Micro-Varianten)
- DisplayPort (normale Größe und miniDP)
- Thunderbolt (inklusive mDP Thunderbolt 1 und 2 und Thunderbolt 3 über USB-C)

Viele Grafikkarten (insbesondere ältere) besitzen zusätzliche Anschlüsse, um Fernsehgeräte, Camcorder oder andere Multimediageräte anzuschließen. Die Grafikkarte in Abbildung 17.39 besitzt drei Anschlüsse: VGA, DVI-I und S-Video. Bevor es HDMI gab, war S-Video eine tolle (oder vielleicht besser: brauchbare) Möglichkeit, einen Fernseher am Computer anzuschließen.

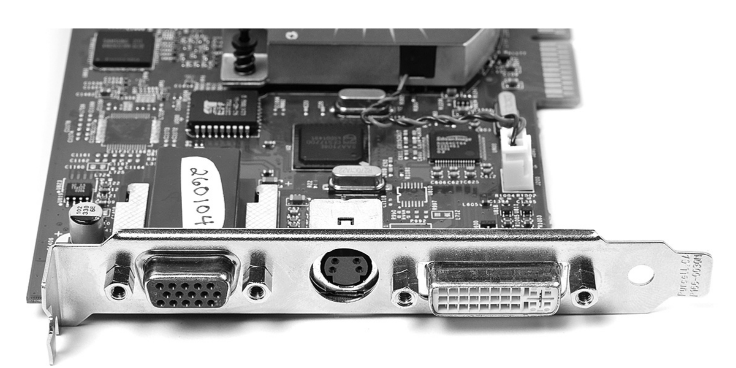


Abb. 17.39: Grafikkarte mit VGA-, S-Video und DVI-I-Anschlüssen

Die Grafikkarte in Abbildung 17.40 hingegen bietet fünf Anschlüsse: DVI, HDMI, DP (drei Mal). Und falls Sie sich das gefragt haben: Ja, die Grafikkarte kann tatsächlich fünf Monitore gleichzeitig ansteuern.

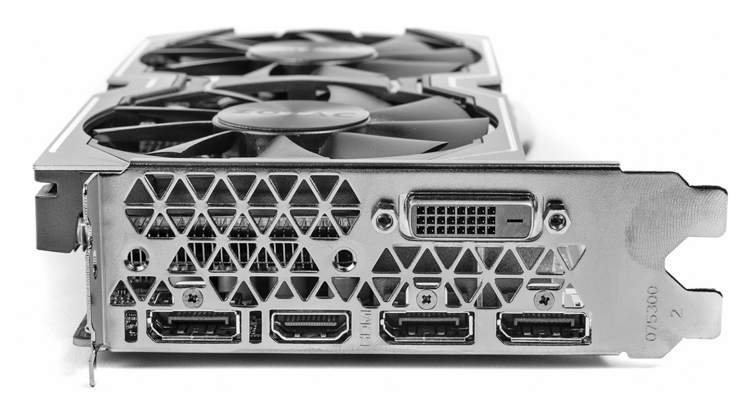


Abb. 17.40: Grafikkarte mit DVI-, HDMI- und DisplayPort-Anschlüssen

17.3 Grafikkarten installieren und konfigurieren

Nachdem Sie entschieden haben, welche Funktionen und welchen Preis Ihre neue Grafikkarte oder Ihr neuer Bildschirm haben soll, müssen Sie diese nur noch in Ihrem System installieren. Wenn es den passenden Anschluss an der Grafikkarte gibt, ist der Anschluss des Monitors ganz einfach. Etwas schwieriger gestaltet sich die Installation der Grafikkarte.

Hinweis

Die Installationsanleitung in diesem Abschnitt bezieht sich auf Windows-PCs und Linux-Rechner. Apple bietet derzeit keine Systeme mit macOS für Endkunden an, bei der die Grafikkarte aufgerüstet werden kann. Sie können diese jedoch konfigurieren oder eine externe GPU anschließen (siehe »eGPUs« im Abschnitt *Jenseits von A+*).

Beim Einbau der Grafikkarte müssen Sie auf drei mögliche Probleme achten: lange Karten, den Abstand zur nächstgelegenen Erweiterungskarte und das Vorhandensein von Stromanschlüssen. Einige der teuren Grafikkarten passen einfach nicht in bestimmte Gehäuse oder blockieren den Zugang zu wichtigen Mainboard-Anschlüssen, wie etwa den SATA-Anschlüssen. Für derartige Probleme gibt es keine einheitliche Lösung. Dann kommen Sie nicht umhin, eine der Komponenten auszutauschen (Grafikkarte, Mainboard oder Gehäuse). Weil qualitativ hochwertige Grafikkarten oft sehr heiß werden, sollten Sie diese auch nicht direkt neben einer anderen Karte platzieren. Sorgen Sie dafür, dass der Lüfter auf der Grafikkarte ausreichend Lüftungsraum erhält. Dabei ist es sinnvoll, den Steckplatz neben der Grafikkarte frei zu lassen, um für einen besseren Luftstrom zu sorgen (Abbildung 17.41).

Viele Premiumgrafikkarten besitzen eingebaute Lüfter, sind aber auch doppelt so breit wie normale Steckkarten. Hier haben Sie keine andere Wahl, als den zweiten Steckplatz aufzugeben. Mittelklasse- oder Spitzengrafikkarten benötigen häufig mindestens einen zusätzlichen PCIe-Stromanschluss, weil sie mehr Strom benötigen, als der PCIe-Steckplatz liefern kann. Vergewissern Sie sich, dass Ihr Netzteil den erforderlichen Strom überhaupt bereitstellen kann und über freie PCIe-Stromanschlüsse verfügt.

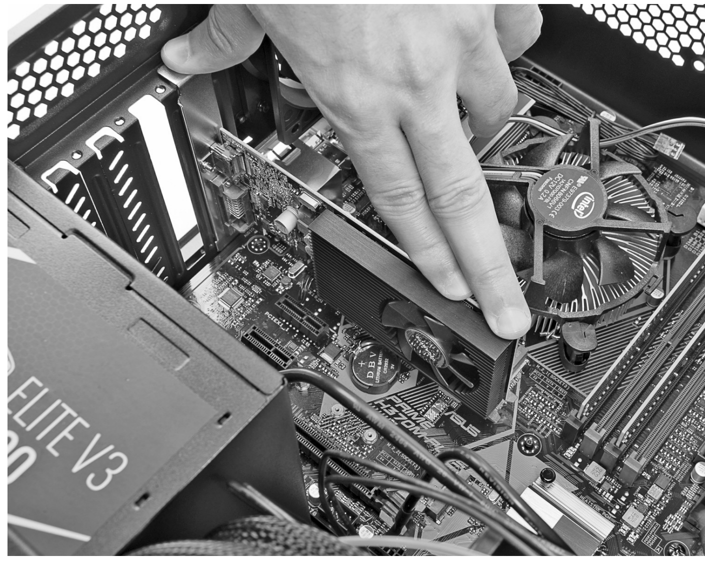


Abb. 17.41: Einbau einer Grafikkarte

Tipp: Einbauen einer Grafikkarte

Wie man eine Erweiterungskarte installiert, wissen Sie aus den vorhergehenden Kapiteln. Gehen Sie beim Installieren auf dieselbe Weise vor:

1. Lesen Sie in Kapitel 6 die Schritte zur Installation einer neuen Erweiterungskarte nach. In Kapitel 7 finden Sie Abbildungen der gängigen Stromanschlüsse.
2. Schließen Sie das Monitorkabel an der Grafikkarte auf der Rückseite des PCs an und starten Sie das System. Wenn der Rechner nicht hochfährt oder der Rechner kein Bild zeigt, obwohl die Lüfter laufen und der interne Lautsprecher ein akustisches Signal (lang-kurz-kurz-kurz) von sich gibt, sitzt die Grafikkarte vermutlich nicht richtig im Steckplatz. Trennen Sie den Rechner vom Stromnetz und probieren Sie den Einbau erneut.

Nachdem Sie die Grafikkarte korrekt installiert und an den Bildschirm angeschlossen haben, ist die Hälfte schon geschafft. Sie müssen nur noch die Treiber installieren und für die passenden Einstellungen im Betriebssystem sorgen, also los!

17.3.1 Software

Die Softwarekonfiguration erfolgt normalerweise in zwei Schritten. Zuerst müssen Sie die Treiber für die Grafikkarte laden. Anschließend starten Sie die Systemsteuerung und dort das Applet ANZEIGE (Windows 7/8/8.1) bzw. öffnen die Einstellungen für die Anzeige (Windows 10), um Ihre Anpassungen vorzunehmen. Jetzt wollen wir uns ansehen, wie die Grafikkarte und der Bildschirm unter Windows in Betrieb genommen werden, und werfen dann kurz einen Blick auf die Anzeigeoptionen in macOS und Linux.

Treiber

Wie alle anderen Hardwarekomponenten ist auch die Grafikkarte auf Treiber angewiesen, um funktionieren zu können. Die Treiber von Grafikkarten werden weitgehend wie die bereits beschriebenen anderen Treiber installiert: Entweder befindet sich bereits ein Treiber im Lieferumfang von Windows oder Sie müssen die mit der Grafikkarte gelieferte Installations-CD bzw. einen aus dem Internet heruntergeladenen Treiber benutzen.

Die Hersteller von Grafikkarten aktualisieren laufend ihre Treiber. Daher ist es sehr wahrscheinlich, dass für Grafikkarten, die bereits einige Monate alt sind, zumindest eine aktualisierte Treiberversion erhältlich ist. Daher sollten Sie möglichst die aktuellen Treiber von der Website des Herstellers benutzen, sofern solche verfügbar sind. Wenn auf der Website keine Treiber angeboten werden, dann verwenden Sie am besten die Treiber von der Installations-CD. Meiden Sie möglichst die Verwendung der Treiber aus dem Lieferumfang von Windows, da diese meist veraltet sind.

Auf Treiberaspekte werde ich ausführlicher nach der Beschreibung des Applets ANZEIGE bzw. ANPASSUNG eingehen. Wie viele andere Dinge im Zusammenhang mit dem Grafiksystem können Sie das eine Thema nicht vollständig verstehen, ohne zuvor nicht zumindest ein anderes verstanden zu haben!

1002

Das Applet Anzeige/Einstellungen der Anzeige

Wenn die Treiber installiert sind, dann können Sie die Anzeigeeinstellungen konfigurieren. Das Applet ANZEIGE in der Systemsteuerung bzw. in der Einstellungs-App bietet praktischen, zentralen Zugang zu allen Anzeigeeinstellungen, wie z.B. der Auflösung, der Bildwiederholrate, den Treiberin-

formationen und der Farbtiefe. Hier konzentrieren wir uns auf Windows 10. Die beiden Versionen unterscheiden sich in der Optik, bieten aber die gleichen Optionen.

Abbildung 17.42 zeigt die Einstellungen der Anzeige für ein System mit zwei Bildschirmen. Jedem angeschlossenen Monitor ist eine Zahl zugeordnet. Die Anordnung der Bildschirme können Sie per Drag&Drop ändern. Abbildung 17.43 zeigt ein System, bei dem die Monitore übereinander angeordnet sind.



Abb. 17.42: Einstellungen Anzeige in Windows 10

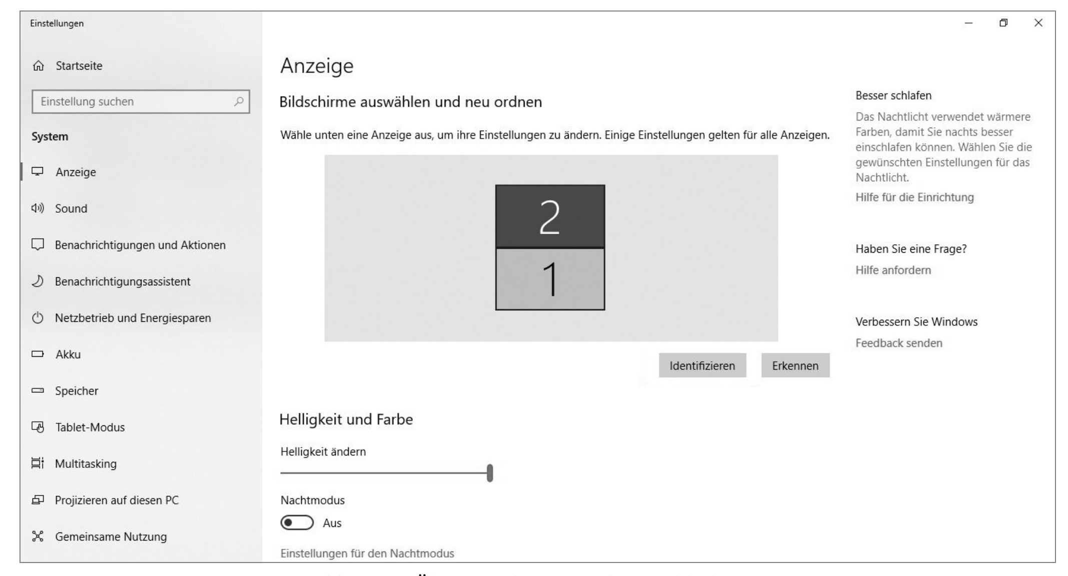


Abb. 17.43: Übereinander angeordnete Bildschirme

Die Optionen darunter sind der Nachtmodus und ein Farbprofil. Wenn der *Nachtmodus* aktiviert ist, werden die Augen geschont, falls man noch arbeitet oder spielt, wenn es bereits dunkel ist. Der Anteil des blauen Lichts der Anzeige wird dann allmählich reduziert, und »Weiß« wird zu einem blassen Orange. Das gehört zwar nicht zur Prüfung, ist aber ein nützliches Feature. Das Farbprofil ermöglicht es, ein Profil mit bestimmten Parametern für einen Bildschirm auszuwählen, damit die auf dem Bildschirm angezeigten Farben mit den gedruckten Farben übereinstimmen – sofern auch der Drucker korrekt farbkalibriert ist. Wenn Windows das Profil automatisch einrichtet, ist das Farbprofil ausgegraut. Sehen Sie sich das Applet FARBVERWALTUNG an, um weitere Einstellungen vorzunehmen (Abbildung 17.44).

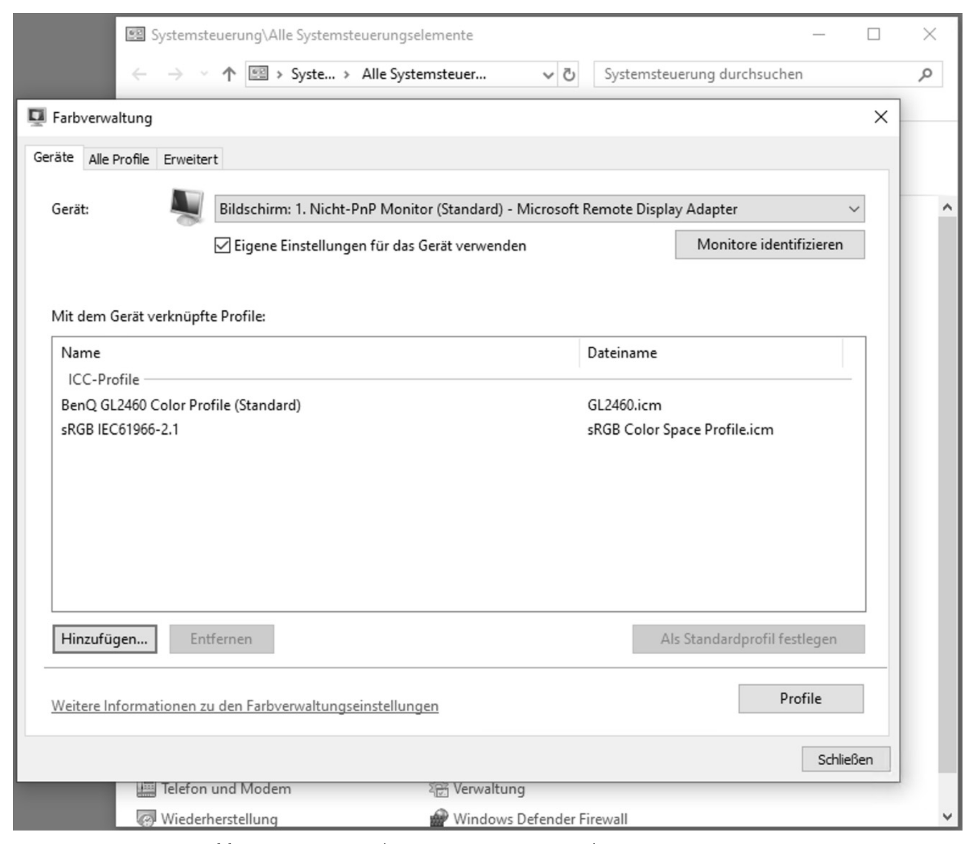


Abb. 17.44: Das Applet FARBVERWALTUNG in der Systemsteuerung

Wenn Sie weiter herunterscrollen, gelangen Sie zu erweiterten Einstellungen (Abbildung 17.45). Sie können die Größe von Text, Symbolen und anderen Elementen durch Einblendmenüs ändern. Das ist bei hochauflösenden Monitoren hilfreich, wenn der Benutzer die Objekte gern ein bisschen größer hätte, um leichter navigieren zu können. Das Skalieren ist dem Ändern der Auflösung vorzuziehen, weil die Bedienoberfläche auf diese Weise die Standardauflösung (und damit die beste) beibehält.

Unter bestimmten Umständen müssen Sie die Auflösung oder die Ausrichtung des Bildschirms ändern. Das Einblendmenü BILDSCHIRMAUFLÖSUNG ermöglicht es, die Auflösung zu ändern (beispielsweise damit sie mit derjenigen eines Projektors übereinstimmt, sodass eine Präsentation auf dem Bildschirm genauso dargestellt wird wie auf der Leinwand). Mit der Option BILDSCHIRMAUSRICHTUNG können Sie diese von Querformat auf Hochformat umstellen, wenn Sie einen schwenkbaren Monitor verwenden (Abbildung 17.46).

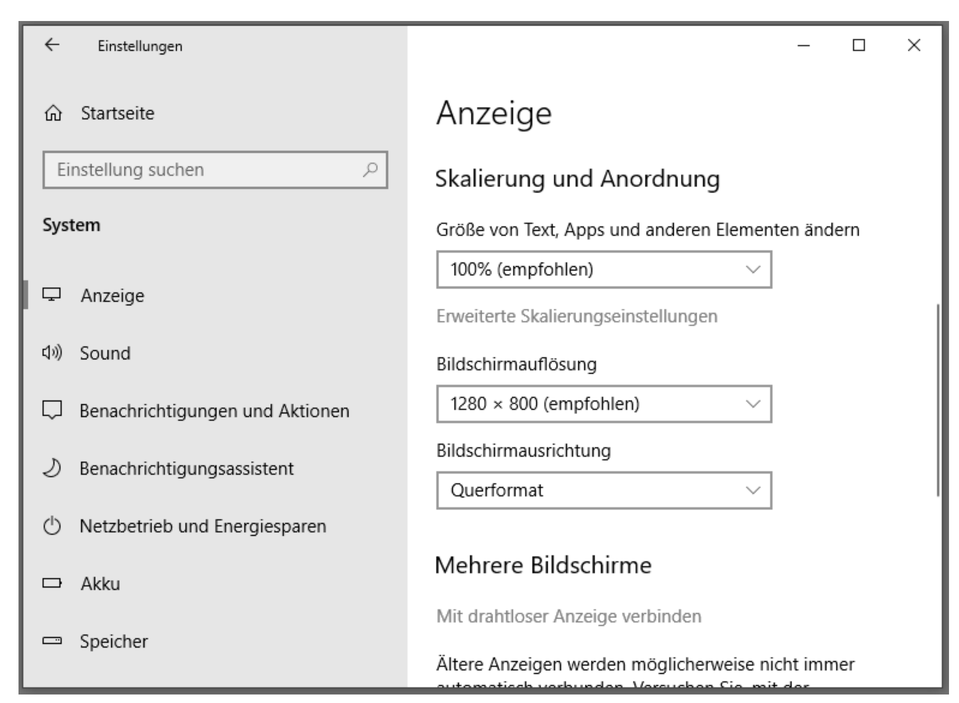


Abb. 17.45: Weitere Einstellungen der Anzeige



Abb. 17.46: Ein Monitor im Hochformat

Die Option MEHRERE BILDSCHIRME gestattet es, festzulegen, was auf dem zweiten (oder dritten, oder vierten ...) Bildschirm angezeigt wird. Voreingestellt ist DIESE ANZEIGEN ERWEITERN. Damit erhalten Sie zusätzlichen Platz auf dem Desktop. Abbildung 17.47 zeigt meinen Redakteur bei der Arbeit an zwei Bildschirmen. Sie können es auch so einrichten, dass alle Bildschirme dasselbe Bild darstellen oder dass einer der Bildschirme leer bleibt.

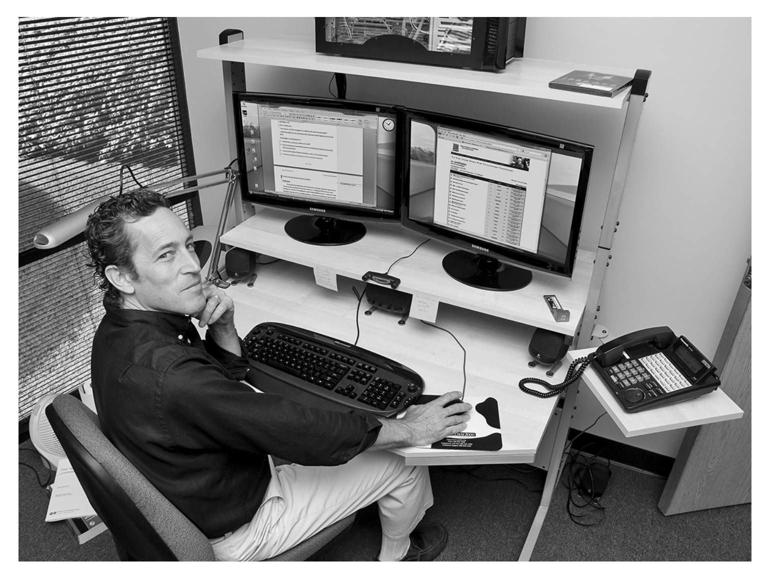


Abb. 17.47: Mein Redakteur bei der Arbeit an zwei Bildschirmen

Hinweis

Heutzutage können Sie meist problemlos weitere Bildschirme zu einem System hinzufügen. Früher musste man eine zweite Grafikkarte installieren, den Monitor daran anschließen und das Applet ANZEIGE öffnen, um diese zu erweitern. Die meisten heute erhältlichen Grafikkarten der Mittelklasse (oder bessere) verfügen über mehr als einen Anschluss, oft auch verschiedenen Typs. Beschaffen Sie sich ein passendes Kabel und schließen Sie einen weiteren Monitor an, um mehr Freude bei der Arbeit mit dem Computer zu haben.

Klicken Sie auf ERWEITERTE ANZEIGEEINSTELLUNGEN, um Informationen über den oder die angeschlossenen Bildschirm(e) zu erhalten. Abbildung 17.48 zeigt die erweiterten Einstellungen. Hier werden Auflösung, Bildwiederholrate und Bittiefe des Bildschirms angezeigt (sowie Farbformat und Farbraum, auf die ich im Abschnitt *Jenseits von A+* zurückkomme).

Hier können Sie auch das Dialogfeld EIGENSCHAFTEN aufrufen, indem Sie auf ADAPTEREIGENSCHAFTEN ANZEIGEN klicken (Abbildung 17.49). Die Registerkarte GRAFIKKARTE zeigt allgemeine Informationen über das Gerät an. Ein Klick auf die Schaltfläche EIGENSCHAFTEN öffnet ein Dialogfeld zum Aktualisieren oder Zurücksetzen des Treibers. Mehr dazu im Abschnitt 17.3.2, *Arbeiten mit Treibern.*

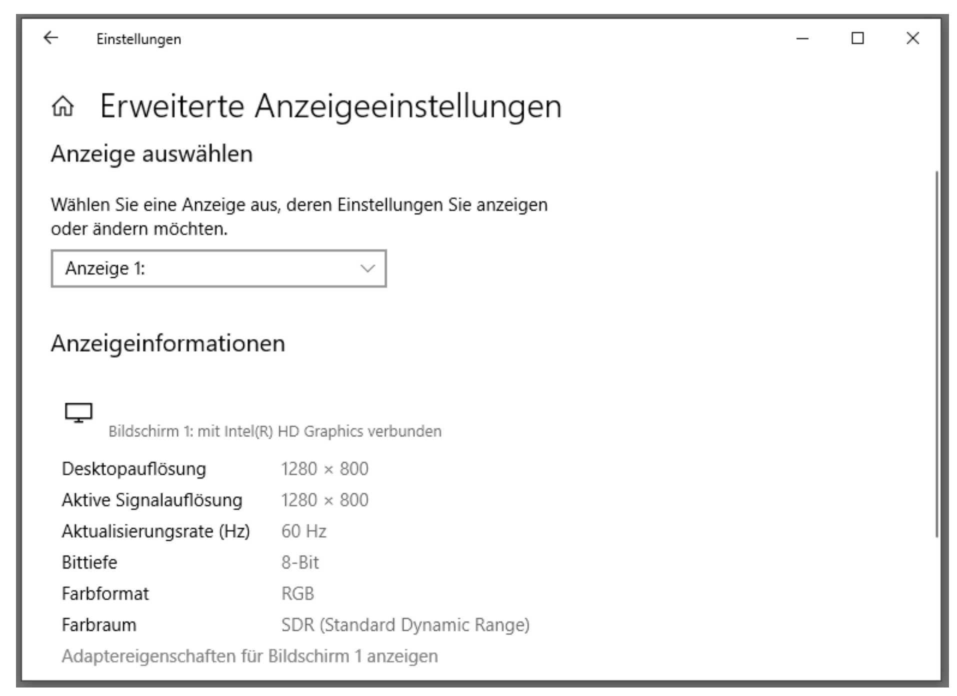


Abb. 17.48: Erweiterte Anzeigeeinstellungen

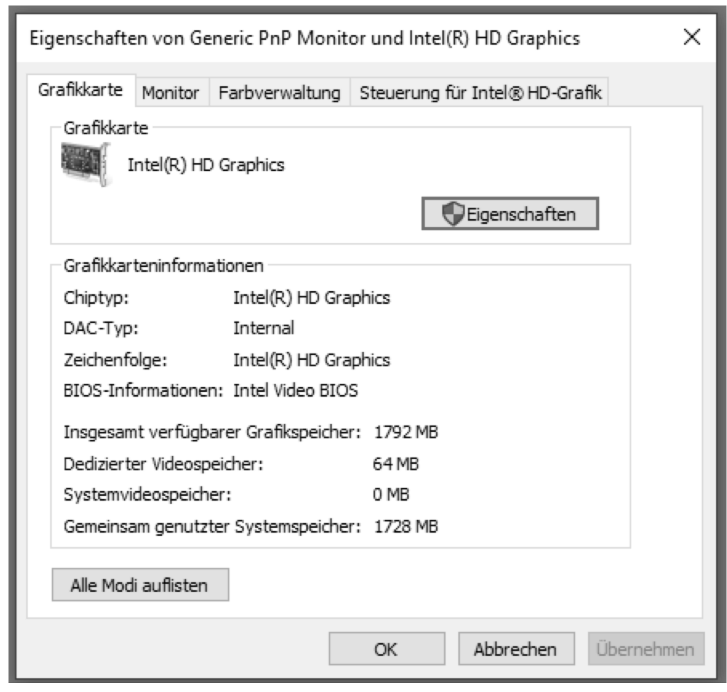


Abb. 17.49: Das Dialogfeld EIGENSCHAFTEN mit den Registerkarten GRAFIKKARTE, MONITOR, FARBVERWALTUNG und einer herstellerspezifischen Registerkarte

Abbildung 17.50 zeigt das Applet ANZEIGE in Windows 8.1. Es bietet im Wesentlichen die gleichen Optionen wie die Einstellungen der Anzeige in Windows 10, sie sind lediglich anders angeordnet.

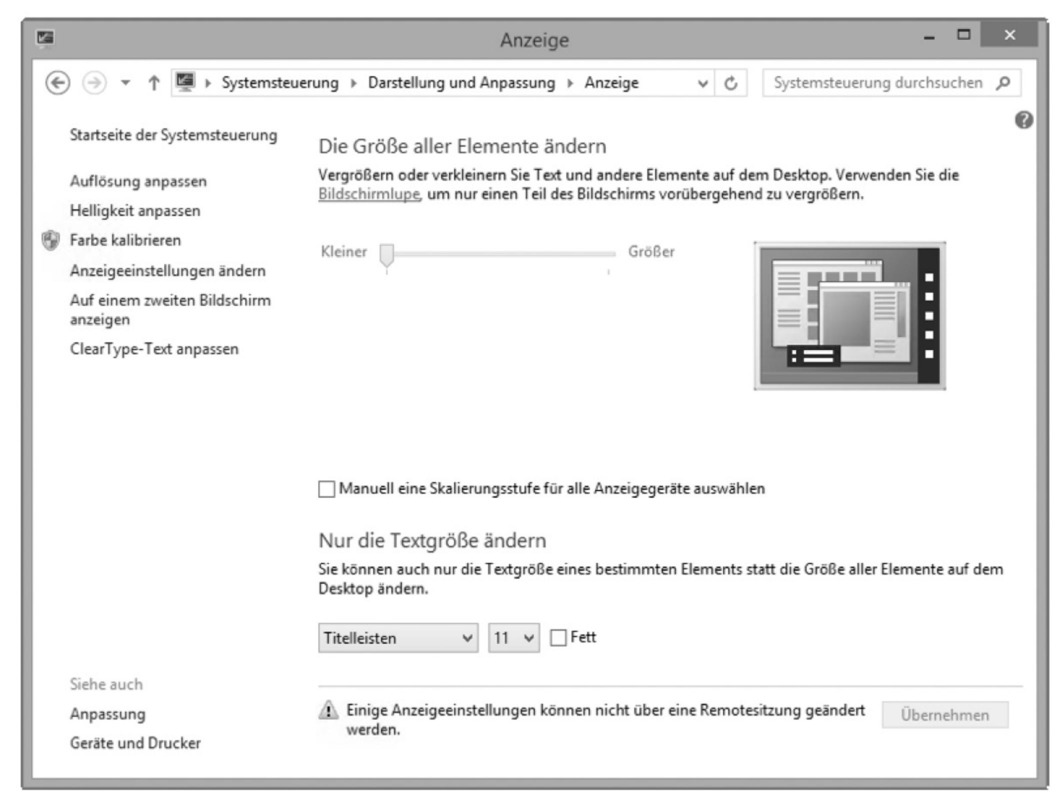


Abb. 17.50: Das Applet ANZEIGE in Windows 8.1

Personalisierung

Durch die Personalisierung werden die Vorlieben des Benutzers berücksichtigt, wie Hintergrundbilder, Farben oder verschiedene Elemente der Bedienoberfläche. Abbildung 17.51 zeigt die Einstellungen zur Personalisierung. Die Änderungen, die Sie vornehmen können, liegen eigentlich auf der Hand: Wählen Sie für den Hintergrund eine Volltonfarbe oder ein Bild aus. Sie können eines der mit Windows ausgelieferten Bilder oder ein eigenes Bild verwenden.

Die Liste auf der linken Seite bietet eine Vielzahl weiterer Möglichkeiten, Windows an Ihre Vorlieben anzupassen, wie die Auswahl vorgefertigter Designs, das Ändern der Standardschrift und die Anpassung des Startmenüs und der Taskleiste. Im unteren Bereich sind EINSTELLUNGEN FÜR HOHEN KONTRAST zu finden, die Menschen helfen können, denen die normale Bedienoberfläche Schwierigkeiten bereitet. Die Option EINSTELLUNGEN SYNCHRONISIEREN ermöglicht die Synchronisierung mehrerer Windows-Rechner, auf denen Sie sich mit Ihrem globalen Microsoft-Benutzerkonto anmelden. Standardmäßig sind alle aktiviert (Abbildung 17.52).

Abbildung 17.53 zeigt das Applet ANPASSUNG in Windows 8.1. Hier gibt es praktisch dieselben Optionen wie in Windows 10, die nur anders angeordnet sind.

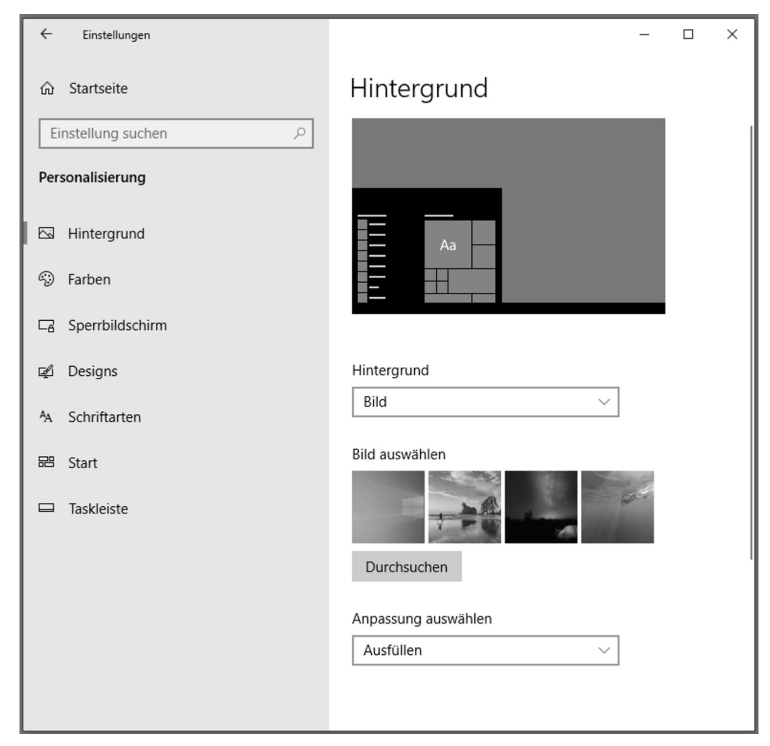


Abb. 17.51: Einstellungen zur Personalisierung

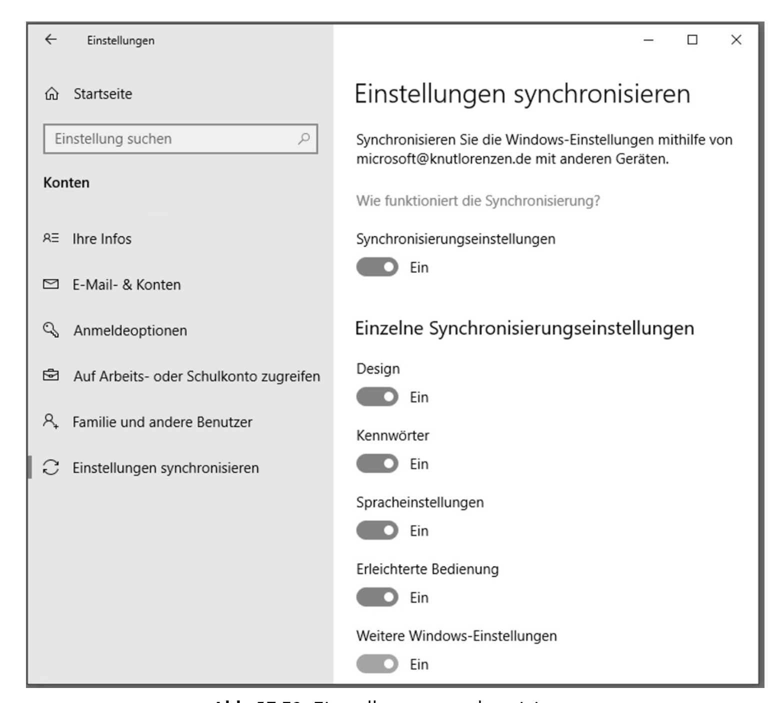


Abb. 17.52: Einstellungen synchronisieren

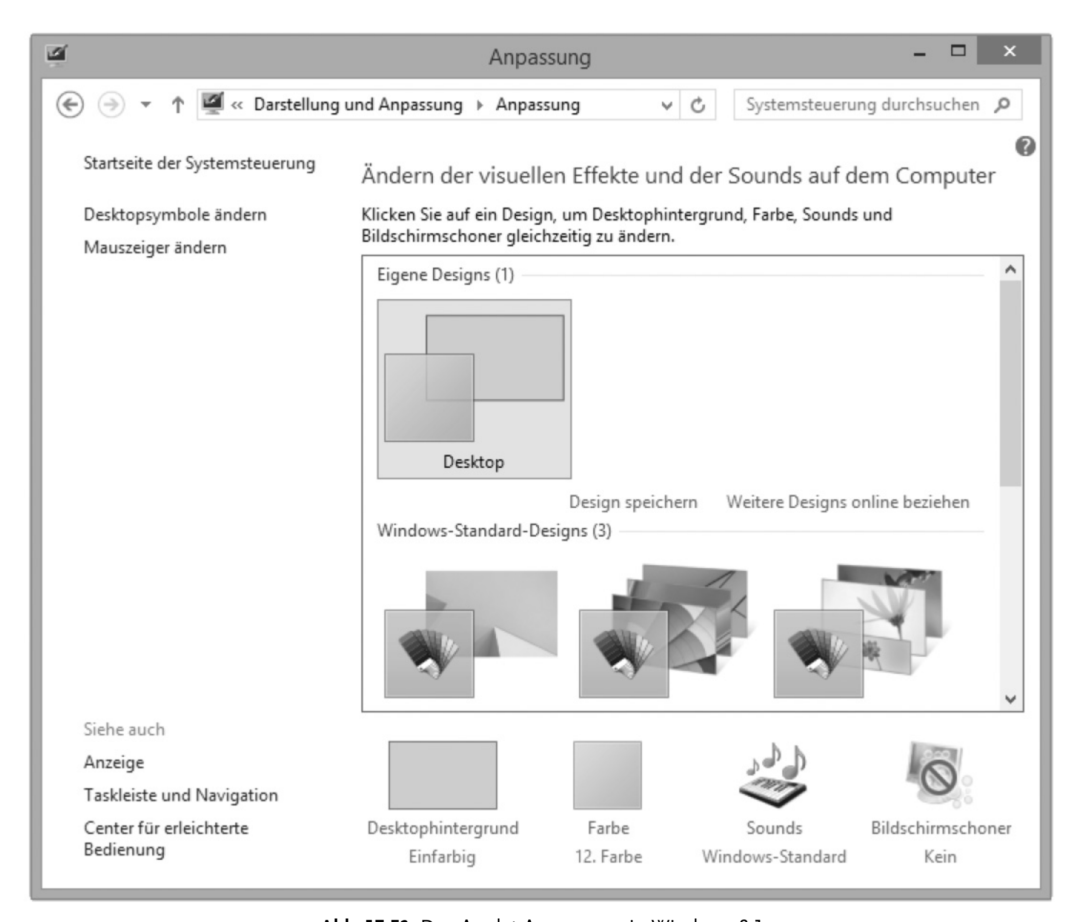


Abb. 17.53: Das Applet ANPASSUNG in Windows 8.1

Anzeigeeinstellungen in macOS und Linux

macOS und die meisten modernen Linux-Distributionen bieten ziemlich unmissverständliche Optionen zum Ändern der Anzeigeeinstellungen. In macOS finden Sie diese erwartungsgemäß in den Systemeinstellungen (Abbildung 17.54). Im Applet ALLGEMEIN ist das farbliche Erscheinungsbild einstellbar. Der Schreibtischhintergrund lässt sich im Applet SCHREIBTISCH & BILDSCHIRMSCHONER ändern.

Klicken Sie auf DOCK, um auf die Einstellungen zuzugreifen, von denen die Benutzererfahrung stark beeinflusst wird (Abbildung 17.55). Das Dock befindet sich standardmäßig am unteren Bildschirmrand. Sie können die Größe der Icons verkleinern, damit sie weniger auffällig sind, die Position des Docks auf dem Bildschirm anpassen oder das Verhalten ändern, wenn der Mauszeiger über dem Dock platziert wird.

Bei den verschiedenen Linux-Distributionen finden sich die Anzeigeeinstellungen an unterschiedlichen Stellen, aber für gewöhnlich erreicht man sie über eines der Werkzeuge in den Systemeinstellungen. Abbildung 17.56 zeigt beispielsweise das Applet in Ubuntu, in dem Sie Schreibtischhintergrund, Thema und Größe der Startersymbole ändern können.

Abb. 17.54: Systemeinstellungen in macOS

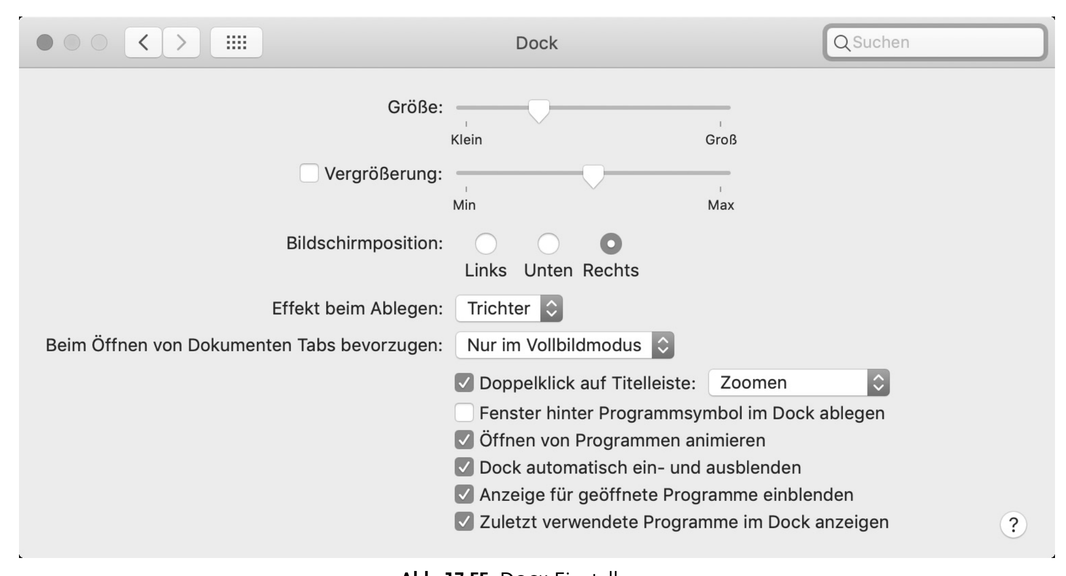


Abb. 17.55: Dock-Einstellungen

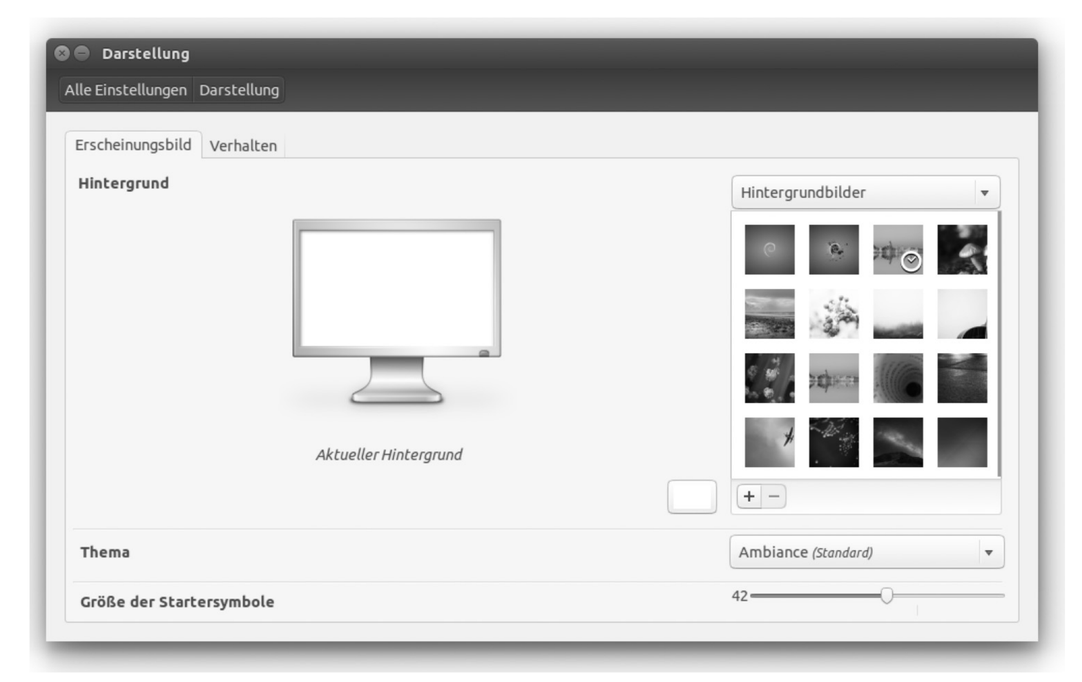


Abb. 17.56: Das Applet DARSTELLUNG der Systemeinstellungen in Ubuntu

Alles, was in Windows einstellbar ist, kann auch in Linux geändert werden – Sie müssen unter Umständen nur ein wenig danach suchen.

17.3.2 Arbeiten mit Treibern

Da Sie nun wissen, wo Sie die wichtigsten Hilfsprogramme für die Anzeige im Betriebssystem finden, ist es an der Zeit, sich mit der Feinabstimmung des Grafiksystems zu befassen. Sie müssen wissen, wie Grafikkartentreiber über das Applet ANZEIGE/ANPASSUNG aktualisiert, wiederhergestellt oder deinstalliert werden können.

Wenn Sie die Treiber einer Grafikkarte aktualisieren, dann können Sie wahlweise erst die alten Treiber deinstallieren, um anschließend die neuen zu installieren. Damit entspricht der Vorgang der Installation einer neuen Karte. Sie können aber auch die digitalen Muskeln ein wenig spielen lassen und neue Treiber direkt über die alten installieren.

Um an die Treibereinstellungen zu gelangen, öffnen Sie die Einstellungen für die Anzeige und klicken zunächst auf ERWEITERTE ANZEIGEEINSTELLUNGEN und dann auf ADAPTEREIGENSCHAFTEN ANZEIGEN, um das Dialogfeld mit den Eigenschaften von Monitor und Grafikkarte aufzurufen. Klicken Sie nun auf der Registerkarte GRAFIKKARTE auf EIGENSCHAFTEN (Abbildung 17.57). Als »Grafikkarte« wird im Dialogfeld nun die ausgewählte Grafikkarte angezeigt. Auf der Registerkarte ALLGEMEIN sind allgemeine Informationen zu finden, aber auf der Registerkarte TREIBER geht es zur Sache.

Um die Treiber zu aktualisieren, klicken Sie die Schaltfläche TREIBER AKTUALISIEREN an, um den Assistenten zu starten. Windows bietet an, sowohl auf Ihrem Computer als auch im Internet oder nur auf Ihrem Rechner nach neuen Treibern zu suchen (Abbildung 17.58). Die erstgenannte Option funktioniert heutzutage fast wie von Zauberhand – sofern der Computer über eine Internetverbindung verfügt.

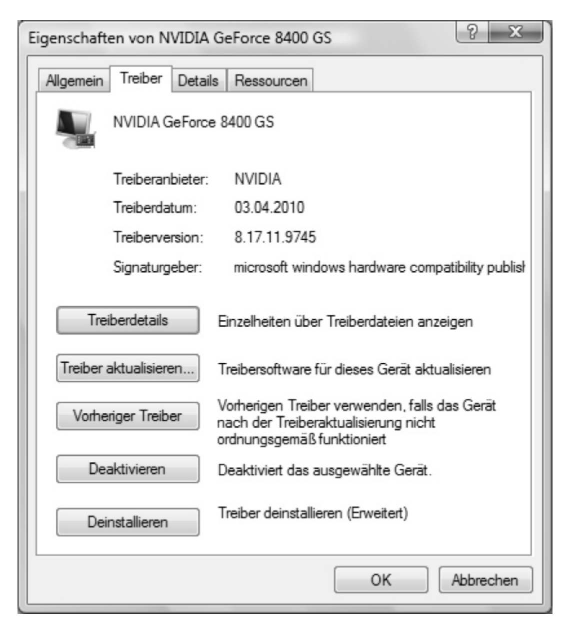


Abb. 17.57: Das Dialogfeld EIGENSCHAFTEN mit ausgewählter Registerkarte TREIBER

Abb. 17.58: Windows sucht nach neuen Treibern.

In älteren Windows-Versionen ist es erforderlich, das Applet ANZEIGE in der Systemsteuerung zu öffnen. Dort gelangen Sie auf dem gleichen Weg zu dem Dialogfeld mit den Eigenschaften, auf dem Sie wie in Windows 10 die Registerkarte TREIBER auswählen. Dort finden Sie dieselben Optionen vor.

Geschichte und Konzepte

17.3.3 3-D-Grafik

Kein anderer Bereich spiegelt die erstaunliche Beschleunigung der technologischen Entwicklungen besser wider als 3-D-Grafiken und insbesondere 3-D-Spiele. Wir sind die Zuschauer einer neuen Welt, in der die Software und die Hardware miteinander darum wetteifern, neue Realitäts- und Komplexitätsebenen zu erreichen und diese auf dem Computerbildschirm darzustellen. Mit dem Geld von Millionen PC-Spielern, die immer neue und bessere Spiele nachfragen, führen Hersteller ständig neue Grafikkarten ein und stellen neue Software vor, die unglaublich realistisch ist und für ungeheuren Spielspaß sorgt.

Auch wenn der Spielesektor der PC-Industrie sicherlich im Bereich der 3-D-Technologien führend ist, greifen viele andere PC-Anwendungen, wie z.B. CAD-Programme (*Computer Aided Design*), diese Technologien auf, sodass 3-D nicht nur im Spielesektor nützlich ist. In diesem Abschnitt werde ich die vielen über die letzten Kapitel verstreuten Fragmente zur 3-D-Grafik aufgreifen und zusammensetzen, damit Sie die Funktionen und die Konfiguration von 3-D-Grafiken besser zu verstehen.

Bis zum Beginn der 1990er-Jahre eigneten sich PCs nicht besonders zur Darstellung von 3-D-Grafiken. Sicherlich gab es bereits viele 3-D-Anwendungen (vorwiegend 3-D-Design-Programme, wie z.B. AutoCAD und Intergraph), aber diese Anwendungen liefen nur auf teurer, spezieller Hardware, was für Gelegenheitsanwender keine wirkliche Alternative war.

Der große Wandel fand 1992 statt, als das kleine Unternehmen id Software ein neues Spiel namens *Wolfenstein 3D* herausbrachte, das eine völlig neue Spielegattung ins Leben rief, die im englischen Sprachraum *first-person shooters* (FPS) genannt wird (Abbildung 17.59). In diesen Spielen dringt der Spieler in eine dreidimensionale Welt ein und interagiert mit Wänden, Türen und Gegenständen und schießt alle bösen Buben über den Haufen, die sich ihm beim Spielen in den Weg stellen.



Abb. 17.59: Wolfenstein 3D

Wolfenstein 3-D erschütterte die PC-Spielewelt bis in ihre Grundfesten. Ein aufstrebendes kleines Unternehmen erschien plötzlich mit diesem neuen Spielformat, sodass Wolfenstein 3-D und id Software quasi über Nacht berühmt wurden. id Software wusste, dass ihr 3-D-Spiel für die damalige Zeit ziemlich hohe Hardwareanforderungen stellte, riskierte es aber und vertraute darauf, dass es genügend leistungsfähige Systeme gab, um das Spiel erfolgreich werden zu lassen. Das Risiko wurde belohnt und machte John Carmack und John Romero, die Gründer von id Software, zu den Vätern der 3-D-Spiele.

In frühen 3-D-Spielen kamen starre 2-D-Bilder (sogenannte *Sprites*) zum Einsatz, aus denen die 3-D-Welt aufgebaut wurde. Ein Sprite ist nichts anderes als eine Bitmap-Grafikdatei. In diesen frühen Spielen wurde die Position eines Objekts aus der Perspektive des Spielers berechnet und ein Sprite zur Darstellung des Objekts platziert. Für die einzelnen Objekte stand nur eine beschränkte Anzahl von Sprites zur Verfügung. Wenn man um ein Objekt herumging, konnte man deutliche Sprünge wahrnehmen, wenn das aktuelle Sprite durch ein anderes an der neuen Position ersetzt wurde. Abbildung 17.60 zeigt verschiedene Sprites desselben bösen Buben in Wolfenstein 3D. Sprites waren nicht gerade schön, funktionierten in Anbetracht der Einschränkungen der damaligen 486er und ersten Pentium-Rechnern jedoch recht gut.





Abb. 17.60: Für die einzelnen Charaktere gab es nur eine beschränkte Anzahl von Sprites

Die zweite Generation von 3-D-Spielen begann, als Sprites durch echte 3-D-Objekte ersetzt wurden, die wesentlich komplexer als Sprites waren. Ein echtes 3-D-Objekt setzt sich aus vielen *Schnittpunktbeschreibungen* (*vertices*; Singular: *vertex*) zusammen. Jeder dieser Schnittpunkte verfügt in einer 3-D-Welt über eine definierte X-, Y- und Z-Position. Abbildung 17.61 zeigt die Schnittpunktbeschreibungen eines Kriegers in einer 3-D-Welt.

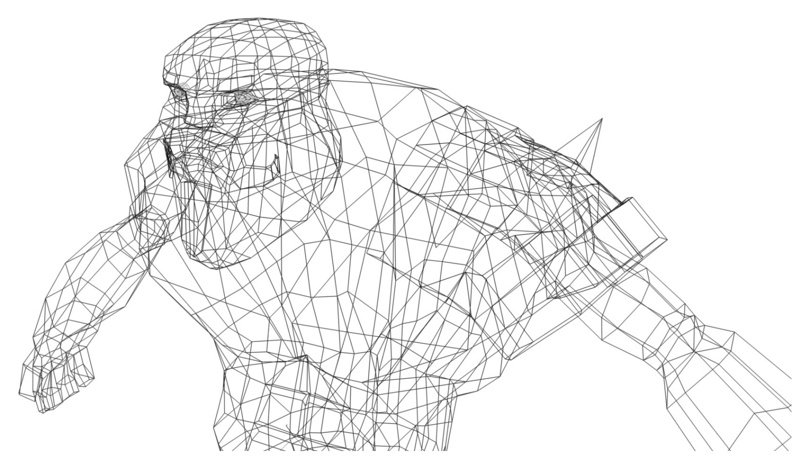


Abb. 17.61: Schnittpunktbeschreibungen eines 3-D-Kriegers

Der Computer muss laufend die Schnittpunkte aller Objekte in der 3-D-Welt aufzeichnen und dabei auch jene erfassen, die aktuell nicht sichtbar sind. Denken Sie daran, dass es in 3-D-Welten bewegungslose Objekte (wie z.B. eine Wand) geben kann, animierte Objekte (wie z.B. eine sich öffnende und schließende Tür) oder sich bewegende Objekte (wie z.B. böse Monster, die versuchen, Sie mit ätzendem Schleim zu bespucken) geben kann. Dieser Berechnungsprozess wird *Transformation* genannt und beansprucht, wie Sie sich sicherlich denken können, die meisten Prozessoren äußerst stark. Intels und AMDs SIMD-Prozessorerweiterungen (SSE usw.) wurden speziell dafür entwickelt, die Berechnung von Transformationen zu beschleunigen.

Wenn der Prozessor erst einmal die Positionen aller Schnittpunkte errechnet hatte, kann das System mit der Darstellung der 3-D-Objekte anfangen. Das Verfahren beginnt mit dem Zeichnen von Linien (*Kanten* bzw. *edges* in 3-D-Terminologie) zwischen den Schnittpunkten, um so das 3-D-Objekt aus vielen Dreiecken aufzubauen. Warum Dreiecke? Nun, vorwiegend wohl, weil die Spiele-Entwickler übereinstimmend der Meinung waren, dass zwar alle geometrischen Formen prinzipiell funktionieren würden, dass sich Dreiecke aus mathematischer Sicht aber am besten eigneten. Wenn ich hier darauf ausführlicher eingehen wollte, müsste ich über Trigonometrie schreiben, und ich möchte wetten, dass Sie derart ausführliche Beschreibungen ohnehin nicht lesen würden! Bei allen 3-D-Spielen werden die Schnittpunktbeschreibungen (vertices) durch Dreiecke verbunden. Das 3-D-Verfahren fasst die Dreiecke dann in verschiedenen Formen, die *Polygone* genannt werden, zu Gruppen zusammen. Abbildung 17.62 zeigt das Modell aus Abbildung 17.61, wobei diesmal alle Schnittpunktbeschreibungen zu einer großen Anzahl von Polygonen verbunden sind.



Abb. 17.62: Die verbundenen Schnittpunkte bilden Polygone auf dem 3-D-Objekt

Ursprünglich übernahm der Systemprozessor diese Berechnungen zum Erzeugen der Dreiecke. Seit der Vorstellung der Grafikkarte GeForce 256 im Jahre 1999 wird diese Aufgabe jedoch von speziellen 3-D-Grafikkarten übernommen, die diesen Vorgang erheblich beschleunigen.

Der letzte Schritt bei den Spielen der zweiten Generation war die *Texturierung*. Alle 3-D-Spiele speichern eine Reihe von Bitmaps, die *Texturen* genannt werden. Das Programm »wickelt« die Texturen um das Objekt, um ihm eine Oberfläche zu geben. Texturen eignen sich hervorragend, denn sie bieten viele Details, ohne dass übermäßig viele Dreiecke berechnet werden müssen. Für einzelne Objekte können eine oder mehrere Texturen verwendet werden, die auf einzelne Dreiecke oder Gruppen von Dreiecken (Polygone) angewandt werden. Abbildung 17.63 zeigt den fertigen Krieger.



Abb. 17.63: 3-D-Krieger mit hinzugefügten Texturen

Echtes 3-D, bei dem eher von »gerenderten« Objekten die Rede ist, sorgte sofort für eine Nachfrage nach überaus leistungsfähigen Grafikkarten und breiteren Datenbussen. Die Entwicklung von AGP durch Intel hatte vorrangig das Ziel, den mittlerweile für Grafikkarten zum Engpass gewordenen PCI-Bus abzulösen und einen Datenpfad zu schaffen, der auch den riesigen, zwischen dem Prozessor und der Grafikkarte zu transportierenden Datenmengen gewachsen war. Intel verlieh AGP die Fähigkeit zum Lesen des System-RAMs, um den zur Unterstützung von Texturen erforderlichen Speicher (auch) auf diesem Weg zur Verfügung stellen zu können. Ohne 3-D-Spiele gäbe es AGP (und wohl auch PCIe) wahrscheinlich nicht.

3-D-Grafikkarten

Mitte der 1990er-Jahre war keine CPU auch nur annähernd in der Lage, die umfangreichen Berechnungen zum Rendern von 3-D-Welten zu bewältigen. Denken Sie daran, dass der Bildschirminhalt auch bei 3-D-Welten mindestens 24 Mal je Sekunde (Bildwiederholrate von Kinofilmen) aufgefrischt werden muss, um realistisch wirkende Bewegungsabläufe darstellen zu können. Der gesamte Prozess von der Transformation bis hin zur Texturierung darf also höchstens 1/24stel-Sekunde dauern! Weiterhin muss das Spiel nicht nur den Bildschirm neu aufbauen, sondern auch die Ereignisse aufzeichnen und z.B. die Position aller Objekte im Spiel notieren und für ein gewisses »intelligentes« Verhalten der bösen Buben sorgen. Es musste einfach etwas zur Entlastung der CPU unternommen werden. Die Lösung konnte nur aus dem Bereich der Grafikkarten kommen.

Es wurden Grafikkarten mit intelligenten Onboard-GPUs (*Graphical Processing Units*) entwickelt. Die GPUs halfen der CPU, indem sie zunächst einige, später sogar alle 3-D-Darstellungen übernahmen. Diese Grafikkarten haben nicht nur GPUs, sondern auch einen riesigen RAM-Speicher, um Oberflächenstrukturen zu speichern.

Ein Problem bleibt bei dieser Konfiguration aber bestehen: Wie lässt sich mit derartigen Grafikkarten kommunizieren? Natürlich benötigt man dafür Gerätetreiber. Wäre es aber nicht toll, wenn man Standardbefehle verwenden könnte, mit denen sich der Prozess weiter beschleunigen ließe? Am besten wäre es, wenn man einen standardisierten Befehlssatz definieren würde, den alle 3-D-Programme bei grundlegenden Aufgaben zur Kommunikation mit 3-D-Grafikkarten verwenden könnten und der aus Befehlen, wie z.B. »zeichne einen Kegel« und »lege Textur 237 über den gerade gezeichneten Kegel« bestünde.

Die Standards der Befehle für Grafikkarten führten zu einer Reihe von *APIs* (*Application Programming Interface* – Schnittstelle für die Anwendungsprogrammierung). Im Wesentlichen handelt es sich bei einer API um eine Bibliothek mit Befehlen, die von den Entwicklern der 3-D-Spiele in ihren Programmen verwendet werden. Das Programm, das die Grafikkarte gerade benutzt, sendet API-Befehle direkt an den Gerätetreiber. Die Gerätetreiber übersetzen die API-Befehle in Kommandos, die von der Hardware der Grafikkarte verstanden wird, und übermitteln sie an diese.

Im Laufe der Zeit wurden mehrere verschiedene APIs entwickelt, wobei es letztlich zwei klare Gewinner gab: *OpenGL* und *DirectX*. Der OpenGL-Standard wurde zwar für Unix-Systeme entwickelt, wurde aber *portiert*, sodass er mit einer Vielzahl von Computersystemen kompatibel ist, zu denen Windows- und Apple-Rechner zählen. Mit zunehmender Nachfrage nach 3-D-Grafik entschloss sich Microsoft selbst zur Teilnahme an dem Wettrennen und entwickelte sein eigenes API, das DirectX genannt wurde. DirectX werde ich im nächsten Abschnitt eingehender behandeln.

Hinweis

Inzwischen sind zwei weitere Standards auf dem Vormarsch. Die Open-Source-Gemeinde hat sich *Vulcan* zu eigen gemacht. Apple setzt auf die hauseigene *Metal-API*.

Obwohl sie eigentlich dieselben Aufgaben erledigen (wie z.B. Befehle übersetzen und sie an den Grafikkartentreiber weiterleiten), unterscheiden sich die verschiedenen APIs ein wenig. In manchen 3-D-Spielen könnte OpenGL beispielsweise mit weniger Rechenleistung ein präziseres Bild als DirectX liefern. Im Allgemeinen werden Sie jedoch kaum einen großen Unterschied zwischen den von OpenGL und DirectX errechneten Bildern erkennen.

1002

DirectX und Grafikkarten

In der guten alten Zeit kommunizierten viele Anwendungen direkt mit einem großen Teil der PC-Hardware und konnten damit, wenn sie nicht sauber programmiert waren, einen Rechner zum Absturz bringen. Microsoft versuchte dieses Problem dadurch zu beheben, dass es die gesamte Hardware unter die Kontrolle von Windows stellte. Den Programmierern gefiel das aber gar nicht, weil Windows der Grafikverarbeitung zu viel zusätzliche Arbeit aufbürdete und den gesamten Programmablauf verlangsamte. Für die anspruchsvollsten Programme, wie z.B. Spiele, eignete sich nur der direkte Hardwarezugriff.

Diese Notwendigkeit, »Windows zu umgehen«, motivierte Microsoft zur Entwicklung einer neuen Reihe von Protokollen, die *DirectX* genannt wurden. Die Programmierer konnten DirectX nutzen, um bestimmte Hardwarekomponenten zu steuern und direkt mit dieser Hardware zu kommunizieren. DirectX bot die für die heute beliebten anspruchsvollen Spiele erforderliche Geschwindigkeit. Das vorrangige Ziel der Entwicklung von DirectX war es, die Ausführung von 3-D-Spielen unter Windows zu ermöglichen. Das heißt nicht, dass sich 3-D-Spiele unter Windows *vor* DirectX nicht ausführen ließen, sondern nur, dass sich Microsoft am API-Rennen vorher nicht beteiligt hatte und nichts damit zu tun haben wollte. Das Ziel von Microsoft bei der Entwicklung von DirectX bestand darin, eine absolut stabile Umgebung zu schaffen, die einen direkten Zugriff auf die Hardware ermöglichte, um 3-D-Anwendungen und 3-D-Spiele unter Windows ausführen zu können.

- Microsoft aktualisiert DirectX regelmäßig, und die neuesten Spiele erfordern die letzte DirectX-Version. Diese wird von Windows automatisch aktualisiert, Sie brauchen also nichts zu unternehmen. Aber wenn Sie wissen möchten, welche DirectX-Version auf einem System installiert ist (weil es in der Zertifizierungsprüfung vorkommen könnte), dann benutzen Sie das *DirectX-Diagnoseprogramm*. Geben Sie unter Windows 10 in das Suchfeld `dxdiag` ein und betätigen Sie [↵], um das Diagnoseprogramm zu starten (Abbildung 17.64).

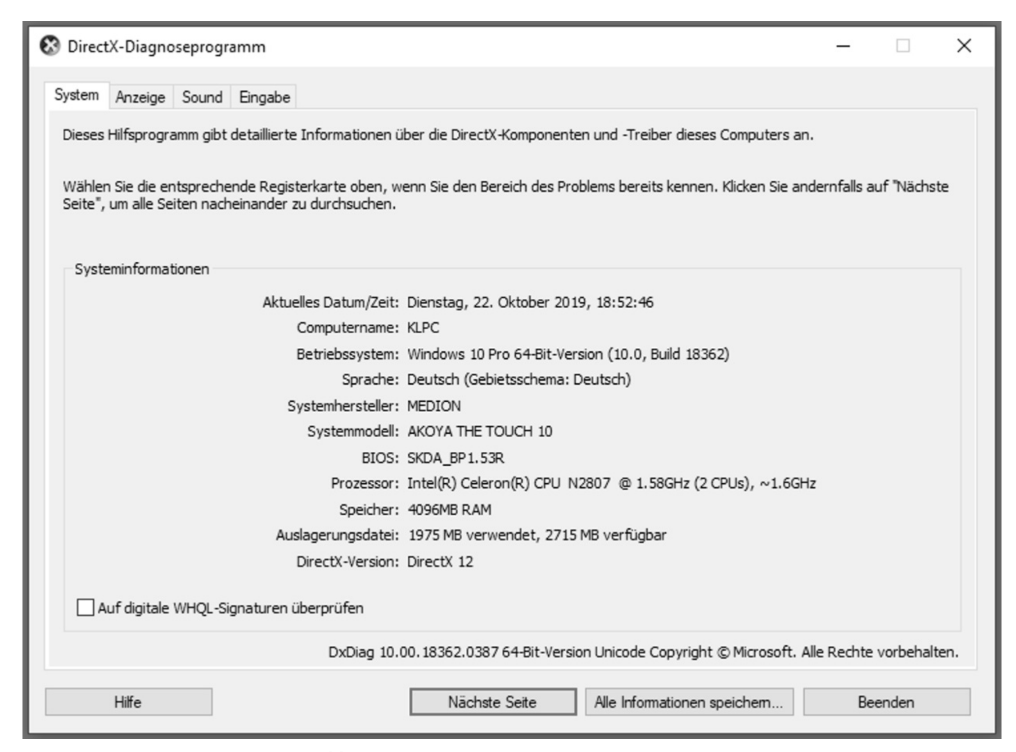


Abb. 17.64: Das DirectX-Diagnoseprogramm

Wichtig

In der CompTIA A+-Prüfung wird das DirectX-Diagnoseprogramm nur als `dxdiag` erwähnt.

Auf der Registerkarte SYSTEM ist die DirectX-Version angegeben. Auf dem in Abbildung 17.64 gezeigten System läuft DirectX 12.

Die Entscheidung über den Kauf einer Grafikkarte lässt mich in Anbetracht der Vielzahl an Optionen buchstäblich schaudern! Beim Kauf einer neuen Grafikkarte ist es aber sicherlich ratsam, sich jeweils darüber zu informieren, welche Grafikchips aktuell angesagt sind. Ich besuche zu diesem Zweck die folgenden Websites, um Testberichte einzusehen:

- `www.arstechnica.com`
- `www.hardocp.com`
- `www.tomshardware.com`
- `www.anandtech.com`

Tipp

Sehen Sie sich die Übung zu `dxdiag` im Abschnitt über Kapitel 17 unter `http://totalsem.com/100x` an. Damit sind Sie auf Prüfungsfragen zum Thema Grafikleistung bestens vorbereitet.

17.4 Problembehebung beim Anzeigesystem

Die Benutzer erkennen sofort, wenn ihr Bildschirm den Windows-Desktop nicht mehr anzeigt, weshalb Grafikprobleme für Techniker von größter Wichtigkeit sind. Ein defekter Drucker oder andere defekte Geräte werden von den Benutzern möglicherweise vorübergehend ignoriert, aber wenn der Bildschirm nicht mehr wie gewünscht funktioniert, dann machen sie einen Aufstand. Um Grafikprobleme schnell zu beheben, beginnen Sie am besten damit, sie in zwei Kategorien einzuteilen: Grafikkarten/Treiber und Bildschirme.

17.4.1 Fehlersuche bei Grafikkarten/Treibern

Grafikkarten gehen nur selten kaputt, die meisten Probleme werden durch inkompatible Treiber oder fehlerhafte Einstellungen verursacht. Vergewissern Sie sich immer, dass Sie den richtigen Treiber installiert haben. Wenn Sie einen nicht kompatiblen Treiber einsetzen, zeigt Windows beim Laden einen Blue Screen. Wird ein Treiber plötzlich beschädigt, zeigt sich dieses Problem normalerweise erst beim nächsten Neustart. Wenn Sie ein System mit defektem Treiber starten, kann Windows wie folgt reagieren: in den SVGA-Modus wechseln, den Bildschirm leer lassen, abstürzen oder wirre Farbmuster oder ein verzerrtes Bild anzeigen. Manchmal erscheinen auch viel zu große Icons oder sogar ein 3-D-Bild mit eigentümlich deformierter Geometrie.

Egal, was auch ausgegeben wird, booten Sie im abgesicherten Modus und setzen Sie den Treiber zurück oder löschen Sie ihn. Beachten Sie, dass die fortschrittlicheren Grafikkarten ihre Treiber als installierte Programme unter PROGRAMME UND FEATURES anzeigen. Sehen Sie also immer erst dort nach, bevor Sie versuchen, Treiber über den Geräte-Manager zu löschen. Laden Sie den neuesten Treiber herunter und installieren Sie ihn.

Wichtig

In den Lernzielen der CompTIA A+-Prüfung 1002 wird erwähnt, dass defekte Treiber dazu führen können, dass Windows in den VGA-Modus übergeht; das wäre eine Auflösung von 640 x 480 Pixeln. Das war früher einmal so, aber die aktuellen Windows-Versionen wechseln bei Problemen mit dem Treiber zu einer Auflösung von 800 x 600 Pixeln (SVGA). Wundern Sie sich also nicht, wenn bei einer Prüfungsfrage die Antwort »VGA-Modus« die einzig richtige zu sein scheint.

Grafikkarten sind zwar relativ robust, enthalten aber zwei Komponenten, die ausfallen können: Lüfter und RAM. Glücklicherweise führt ein Defekt bei einer der beiden Komponenten zu den gleichen bizarren Ausgaben auf dem Bildschirm, nach denen kurz darauf die Bildschirmanzeige einfriert. Normalerweise läuft Windows weiter. Sie können mit Ihrem Mauszeiger weiter auf dem Bildschirm zeigen und die Fenster aktualisieren sich, aber auf dem Bildschirm wird nur ein gewaltiges Chaos angezeigt (Abbildung 17.65).

Fehlerhafte Treiber können dieses Fehlerbild gelegentlich ebenfalls verursachen, wechseln Sie also immer erst in den abgesicherten Modus, um festzustellen, ob das Problem dort auch noch besteht. Falls nicht, gibt es auch kein Problem mit der Grafikkarte!

Wichtig

In den Lernzielen der CompTIA A+-Zertifizierungsprüfung 1001 wird das mehrfache Auftreten von Fehlermeldungen in den Protokolldateien als mögliches Symptom für Probleme mit der Grafikkarte oder den Treibern genannt. Wenn die Grafik Ihnen Schwierigkeiten bereitet und die anderen hier aufgeführten Schritte keine Abhilfe schaffen, sollten Sie einen Blick auf die Protokolldateien des Systems werfen (in der Ereignisanzeige) und prüfen, ob es dort irgendwelche Hinweise gibt. Rechnen Sie damit, dass es in der Prüfung Fragen zum Thema Probleme mit der Grafik und Protokolldateien gibt.

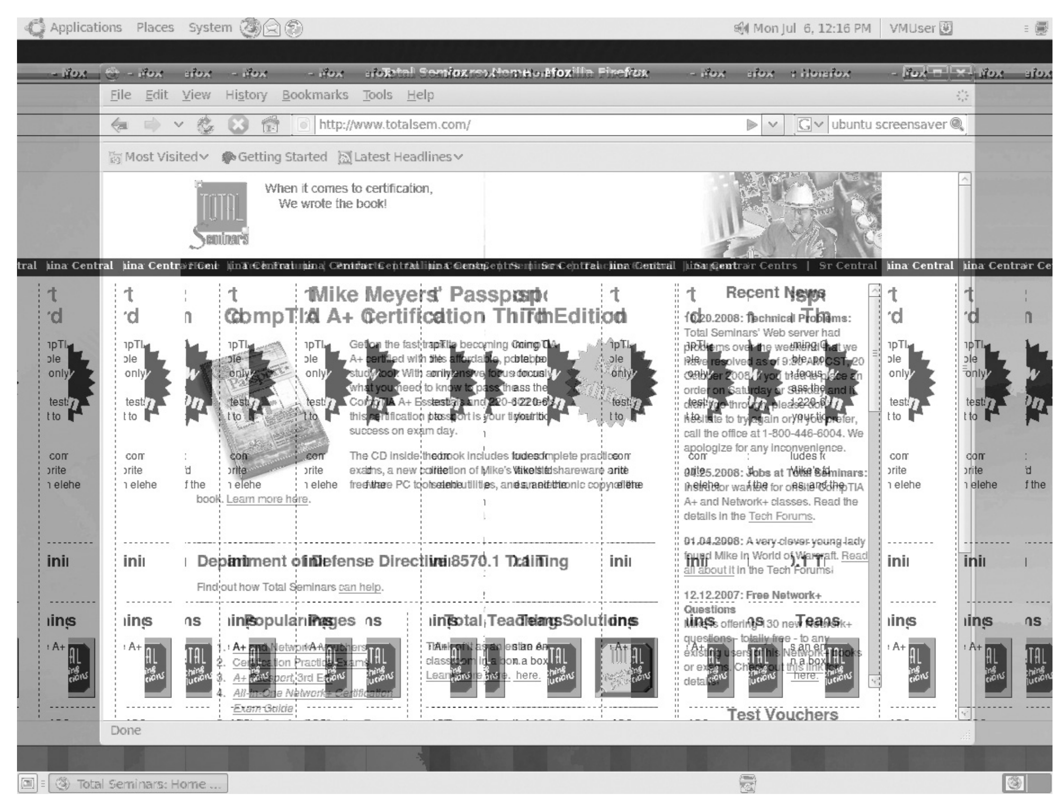


Abb. 17.65: Hier besteht ein ernsthaftes Problem mit der Anzeige.

Wenn das Innere des Computergehäuses zu warm ist, kann es trotz mit Höchstgeschwindigkeit laufender Lüfter ebenfalls zu interessanten Effekten kommen. Der Computer schaltet sich wegen Überhitzung einfach ab. Sie erkennen diese mögliche Ursache daran, dass der Rechner nach dem Wiedereinschalten sich nach einer Minute oder zwei erneut abschaltet, wenn Sie ihn mit Arbeit belasten und er sich erneut überhitzt. Manchmal gibt es auch seltsame grafische Überbleibsel oder Verzerrungen auf dem Bildschirm. Überprüfen Sie Ihre Lüfter und stellen Sie sicher, dass sich keine anderen Komponenten zu nah an der Grafikkarte befinden. Gegebenenfalls müssen Sie Lüfter, Lüftungsschlitze und Gebläse (draußen!) mit Pressluft reinigen.

17.4.2 Fehlersuche bei Bildschirmen

Weil die hohen Frequenzen und Spannungen, mit denen Bildschirme arbeiten, sehr gefährlich sein können und weil für eine korrekte Einstellung eine spezielle Ausbildung erforderlich ist, konzentriert sich dieser Abschnitt darauf, wie Sie einem Support-Fachmann die erforderlichen Informationen bereitstellen, damit dieser für eine Reparatur sorgen kann. Fast kein Bildschirmhersteller stellt heute mehr die Schaltpläne öffentlich zur Verfügung, hauptsächlich wegen Haftungsproblemen bei Personenschäden durch Stromschläge. Um die Fehlersuche zu vereinfachen, betrachten Sie den Prozess in drei Stufen: allgemeine Bildschirmprobleme, externe Einstellungen und interne Einstellungen.

Typische Monitorprobleme

Auch wenn ich mich nicht recht wohlfühle, wenn es an das Eingemachte im Zusammenhang mit Bildschirmen geht, können Sie doch einen großen Teil der Monitorprobleme selbstständig beheben. Die

folgende Liste beschreibt die häufigsten und gibt Ihnen Hinweise zu deren Behebung, selbst wenn das heißt, dass Sie den Monitor zur Reparatur einsenden.

- Bei Problemen mit Geisterbildern, Streifen und/oder unscharfen vertikalen Kanten sollten Sie die Kabelverbindungen und das Kabel selbst überprüfen. Die Ursache derartiger Probleme liegt nur selten beim Monitor selbst. Viel häufiger stellt die Grafikkarte das Problem dar.
- Wenn eine Farbe ausfällt, sollten Sie das Kabel daraufhin überprüfen, ob es Brüche aufweist oder ob einzelne Anschlusspins des Steckers verbogen sind. Prüfen Sie die Steuerelemente bzw. Einstellmöglichkeiten für diese Farbe an der Vorderseite des Monitors. Wenn sich die Farbregulierung bereits am Anschlag befindet, sind interne Wartungsarbeiten erforderlich.
- Wenn Monitore altern, verlieren sie an Helligkeit. Wenn der Helligkeitsregler komplett aufgedreht ist, das Bild aber immer noch zu dunkel scheint, sind interne Einstellungen am Monitor erforderlich. Das ist ein starkes Argument für Energieverwaltungsfunktionen. Nutzen Sie die Energieoptionen von Windows, um den Monitor nach einer bestimmten Zeit auszuschalten oder schalten Sie ihn einfach selbst ab.
- Ein LCD-Bildschirm kann fehlerhafte Pixel aufweisen. Dabei handelt es sich um ein einzelnes Pixel, das nicht so reagiert, wie es sollte. Es kann vorkommen, dass ein Pixel überhaupt nicht leuchtet (totes Pixel), dass es immer weiß bleibt oder stets nur in einer bestimmten Farbe leuchtet. Derartige Pixelfehler können nicht repariert werden. Wenn Sie Pixelfehler bei einem Monitor entdecken, der noch unter Garantie steht, sollten Sie den Hersteller kontaktieren. Falls die Garantie bereits abgelaufen ist, können Sie versuchen, die defekten Pixel durch online beschriebene Verfahren »wiederzubeleben«, die defekten Pixel einfach hinnehmen, oder den Bildschirm ersetzen. Die LCD-Hersteller haben vereinbart, dass selbst auf völlig neuen LCD-Bildschirmen eine bestimmte Anzahl defekter Pixel zulässig ist. Lesen Sie in der Garantie für Ihren Bildschirm nach, um festzustellen, wie viele fehlerhafte Pixel zulässig sind, bevor Sie den Bildschirm zurückgeben.
- Ein zerbrochener LCD-Bildschirm ist irreparabel und muss ersetzt werden.
- Ein flackerndes Bild weist entweder auf ein sehr billiges Panel hin, bei dem zu viel Licht von der Hintergrundbeleuchtung nach außen dringt, oder zeigt an, dass die Kaltkathodenlampe im Begriff ist, ihren Geist aufzugeben. LEDs flackern nicht, bei diesem Bildschirmtyp tritt dieses Phänomen daher nicht auf. Nach Meinung der CompTIA sollten Sie die Kaltkathodenlampe ersetzen, falls erforderlich. Ich empfehle, den Monitor durch ein aktuelles Modell zu ersetzen.
- Ein dunkles Bild, insbesondere nur im oberen oder unteren Bereich der Anzeige, deutet auf eine defekte Hintergrundbeleuchtung hin.
- Wenn Ihr LCD-Bildschirm nicht mehr leuchtet, Sie aber bei hellem Umgebungslicht noch ein Bild sehen können, sind entweder die Lampe oder der Inverter kaputtgegangen. In vielen Fällen, insbesondere bei superflachen Panels, ersetzen Sie das gesamte Panel und die Lampe als Einheit.
- Wenn Ihr LCD-Monitor eine Art zischendes Geräusch von sich gibt, wird der Inverter bald ausfallen. Auch hier lässt sich notfalls wieder der Inverter austauschen.
- Wenn ein Bild sehr lange dargestellt wird, wie es bei vielen Elementen der Bedienoberfläche des Betriebssystems der Fall ist, kann es »einbrennen«, also schattenhaft sichtbar bleiben. Solche Probleme sind heutzutage meist vorübergehender Art und verschwinden wieder, wenn Sie den Bildschirm ausschalten und mindestens so lange ausgeschaltet lassen, wie er vorher eingeschaltet war. Ansonsten ist das Bild tatsächlich eingebrannt. Die erste Generation neuer Display-Technologien hat tendenziell mit dem Einbrennen von Bildern zu kämpfen, deshalb ist es nur vernünftig, dem vorzubeugen und das Betriebssystem so zu konfigurieren, dass ein nicht genutzter Bildschirm abgeschaltet oder ein animierter Bildschirmschoner angezeigt wird.

Passen Sie auf, wenn Sie einen LCD-Monitor öffnen, um an seinen Innereien zu arbeiten. Der Inverter könnte Ihnen auf mehrerlei Weise zu schaffen machen. Erstens wird er von elektrischen Schaltkreisen mit Hochspannung versorgt, die Ihnen einen fürchterlichen Schlag versetzen können. Und der Inverter bleibt auch noch etliche Minuten nach der Trennung des Monitors vom Stromnetz geladen. Warten Sie nach dem Ziehen des Netzsteckers also eine Weile. Zweitens werden Inverter ziemlich heiß, sodass Sie sich daran übel verbrennen können. Auch deshalb sollten Sie nach dem Ziehen des Netzsteckers eine Weile warten. Und schließlich könnten auch Sie selbst dem Inverter einen Schlag verset-

zen und ihn dadurch irreparabel beschädigen. Versuchen Sie, elektrostatische Entladungen also mit entsprechenden Vorkehrungen zu verhindern.

Das Fazit hinsichtlich der Reparatur von LCD-Monitoren? Es gibt zwar Unternehmen, die Ersatzteile für LCDs anbieten, deren Reparatur ist aber ziemlich schwierig. Und es gibt Leute, die das für Sie preiswerter und schneller erledigen, als Sie selbst es könnten. Suchen Sie nach Unternehmen, die sich auf die LCD-Reparatur spezialisiert haben. Weltweit gibt es sicherlich Hunderte derartiger Unternehmen.

Skalierung bei hochauflösenden Monitoren

Hochauflösende Monitore sind ein schöner Anblick, aber für manche Benutzer werden die Bedienelemente auf dem Bildschirm – Schaltflächen, Menüs usw. – zu klein dargestellt. Wie Sie wissen, besitzen LCD-Bildschirme eine Standardauflösung. Wenn Sie eine geringere Auflösung verwenden, leidet die Bildqualität darunter. Dennoch tun das viele Benutzer, weil die Bildschirmelemente dann größer dargestellt werden und sich leichter benutzen lassen. Das ist jedoch nicht die Lösung!

Am besten verwendet man in diesem Fall die Einstellungen der Anzeige. Alle Windows-Versionen bieten die Möglichkeit, die Größe der Bedienelemente zu ändern, sodass sie auf dem Bildschirm größer (oder kleiner) dargestellt werden. Die Auflösung ändert sich dabei nicht, sondern nur die Größe der Bedienelemente. Öffnen Sie die Einstellungen der Anzeige. Abbildung 17.66 zeigt die Optionen des Einblendmenüs in Windows. Um die Größe der Anzeige von Text, Apps und anderen Bedienelementen zu ändern, ist nur ein Mausklick erforderlich.

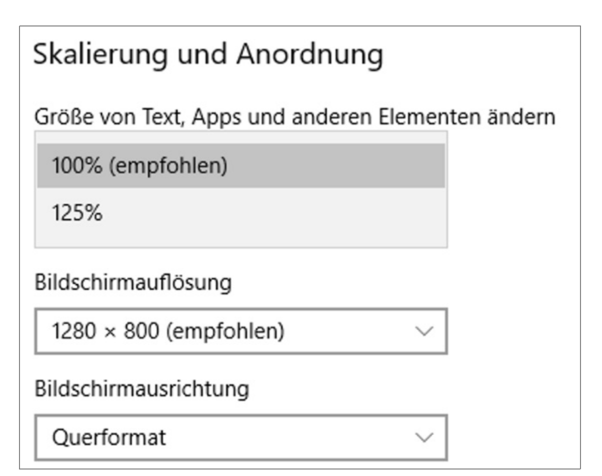


Abb. 17.66: Ändern der Größe von Bedienelementen in Windows 10

Tipp: Skalierung der Bedienelemente

Die meisten Leser können auf einen Windows-Computer zugreifen, also probieren Sie Folgendes aus! Öffnen Sie die Einstellungen für die Anzeige und experimentieren Sie mit der Skalierung der Bedienelemente. Diese Einstellung sollten Sie unbedingt kennen, um Benutzern mit hochauflösenden Monitoren helfen zu können.

Reinigung des Monitors

Die Reinigung von Monitoren ist einfach. Benutzen Sie immer antistatische Tücher. Mikrofasertücher sind dafür bestens geeignet. Für einige LCD-Monitore ist eine spezielle Reinigungsausrüstung erforderlich. Benutzen Sie nie Fensterreiniger oder Flüssigkeiten, da Sie sich der Gefahr von Stromschlägen

aussetzen, wenn Flüssigkeit in den Bildschirm gelangt! Viele der erhältlichen Reinigungslösungen können den Kunststoff eines LCD-Monitors buchstäblich auflösen!

Hinweis

Grafikkarten können mehrere Monitore ansteuern, deren Größe und Auflösung sich unterscheiden, allerdings kann das zu Problemen führen. Wenn Sie bei einer Präsentation einen Projektor mit 4:3-Bildformat an einen Laptop mit Breitbildschirm anschließen, kann das beim Spiegeln des Bildschirminhalts zu ziemlich bizarren Verzerrungen der Darstellung führen. Die Verwendung von Bildschirmen mit unterschiedlicher Ausrichtung (Hoch- und Querformat) kann ebenfalls zu unerwünschten Effekten führen. Probieren Sie das aus, bevor Sie mit der Präsentation anfangen.

Darüber hinaus können Sie in Windows festlegen, welcher Monitor sich links, rechts, oberhalb oder unterhalb des Hauptbildschirms befindet. Wenn man hier einen Fehler macht, kann das beim Erweitern der Anzeige Schwierigkeiten bereiten, beispielsweise wenn Sie den Mauszeiger auf dem linken Bildschirm nach rechts bewegen, dort aber hängen bleiben, weil der vermeintlich rechte Monitor sich tatsächlich auf der linken Seite befindet. Solche Probleme können Sie in den Einstellungen der Anzeige beheben.

Probleme mit mehreren Monitoren

Der Anschluss eines zweiten oder dritten Monitors kann Schwierigkeiten bereiten. Die zusätzliche Anzeigefläche könnte zu Reflexionen oder Spiegelungen anderer Objekte führen, durch die Sie womöglich geblendet werden, wodurch eine optimale Platzierung der Monitore erschwert wird. Sind die Monitore von unterschiedlicher Größe, kann es zu Ausrichtungsfehlern kommen, insbesondere dann, wenn die Monitore verschiedene Standardauflösungen besitzen. Darüber hinaus erleichtern die zusätzliche Anzeigefläche und der erweiterte Blickwinkel es zufällig vorbeikommenden Kollegen, einen Blick darauf zu werfen, was Sie gerade tun oder im Internet betrachten.

Zubehörhändler versuchen, solchen Problemen mit Sichtblenden entgegenzuwirken. Ein solcher Sichtschutz ist exakt an den Bildschirm angepasst und verhindert sowohl seitlichen Einblick als auch unerwünschte Reflexionen.

17.4.3 Fehlersuche bei Projektoren

Viele Konzepte der Fehlersuche bei normalen Bildschirmen behalten auch für die Fehlersuche bei Projektoren ihre Gültigkeit, allerdings sind einige weitere Aspekte zu beachten.

- Die Lampen in Projektoren können *sehr* heiß werden. Lassen Sie, falls möglich, den Projektor abkühlen, bevor Sie sich mit ihm beschäftigen. Nach dem Ausschalten läuft der Lüfter noch eine Weile weiter, um die Lampe abzukühlen. Falls Sie darauf nicht warten können, sollten Sie sehr vorsichtig sein, um Verbrennungen zu vermeiden.
- Projektorlampen haben im Vergleich mit anderen Bauteilen von Anzeigesystemen eine vergleichsweise kurze Lebensdauer (meist ein paar Tausend Stunden). Sie sind teuer, lassen sich aber leicht ersetzen. Halten Sie eine Ersatzlampe bereit. Das rettet Ihnen nicht nur den Tag, wenn vor einem wichtigen Meeting eine Lampe durchbrennt, Sie können bei der Fehlersuche mithilfe der Ersatzlampe auch ausschließen, dass es sich um einen Lampendefekt handelt.
- Wenn wir schon beim Thema Ersatzteile sind: Halten Sie auch Ersatzbatterien für die Fernbedienung des Projektors bereit. Die meisten Projektoren befinden sich an schwer zugänglichen Orten. Wenn das Gerät nicht reagiert, können Sie ausprobieren, die Batterien der Fernbedienung auszutauschen, bevor Sie eine Leiter besorgen müssen, um an die Knöpfe direkt am Projektor zu gelangen.
- Projektoren besitzen einen Lüfter zum Kühlen der Lampe. Wenn der Lüfter ausfällt oder die Lüftungsschlitze blockiert sind, kann sich die Lampe überhitzen. Der Projektor schaltet sich dann möglicherweise automatisch ab. Ihn sofort wieder einzuschalten, um den Fehler zu suchen, funktioniert dann vielleicht überhaupt nicht. Lässt er sich dennoch einschalten, ist das für die Behebung des eigentlichen Problems sicherlich nicht hilfreich.

- Ebenso wie Bildschirme, die längere Zeit nicht benutzt werden, begibt sich ein Projektor möglicherweise in einen Ruhezustand. Normalerweise wacht das Gerät wieder auf, wenn Sie den Computer verwenden oder die entsprechende Taste auf der Fernbedienung betätigen. Wenn der Projektor offensichtlich läuft, aber kein Bild anzeigt, müssen Sie ihn vielleicht neu starten.
- Manche Projektoren setzen ein Farbbild aus mehreren farbigen LCDs zusammen. Wenn die Darstellung falsche Farben enthält oder einen starken Farbstich zeigt, könnte eins der LCD-Panels ausgefallen sein. Wenn bei einem DLP-Projektor die Farben flackern, könnte eines der Farbräder defekt sein.

Vor allem aber sollten Sie sich bei der Fehlersuche nicht *zu sehr* darauf konzentrieren, dass Sie es mit einem Projektor zu tun haben. Man verfällt allzu schnell auf Projektor-spezifische Lösungsversuche und übersieht dabei einfache Probleme, wie ein schlecht verbundenes Kabel oder einen Laptop, der nicht richtig für die Ansteuerung eines Projektors konfiguriert ist.

Jenseits von A+

17.5 Mehr zum Thema Anzeige

Die Anzeige spielt für moderne Computer eine so bedeutende Rolle, dass es kaum zu glauben ist, dass Computer jahrelang verwendet wurden, ohne dass moderne Displays verfügbar waren. Wie schnell Wachstum und Entwicklung der Computertechnologie voranschreiten, zeigt sich nirgendwo deutlicher als bei der Auswahl der verfügbaren besonders dünnen, gekrümmten, extrem hoch auflösenden, extrabreiten, superschnellen, energiesparenden und beeindruckend großen Displays.

Das Tempo der Änderungen von Display-Technologien ist derart hoch, dass man kaum Schritt halten kann. Allerdings kosten viele der Neuerungen ein Vermögen. Ein guter Techniker muss jedoch bei diesen Entwicklungen auf dem Laufenden bleiben, um Displays auswählen zu können, die für die Benutzer sinnvoll sind, und um zu vermeiden, für überflüssige Features Geld aus dem Fenster zu werfen. In diesem Sinne wollen wir einige Themen betrachten, die zwar nicht zur Zertifizierungsprüfung gehören, denen Sie in der Praxis aber sehr wohl begegnen werden: MicroLED-Displays, High Dynamic Range, Adaptive Sync, Grafikmodi und externe GPUs.

17.5.1 MicroLED

Bei einem MicroLED-Monitor (µLED) bilden Gruppen mikroskopisch kleiner LEDs die Pixel, allerdings ist diese Technologie noch nicht reif für die Massenproduktion. MicroLED-Displays sind leistungsfähiger als herkömmliche LCD-Panels. Sie arbeiten energiesparender und bieten größere Helligkeit, höheren Kontrast und kürzere Reaktionszeit. Bei mehreren Unternehmen arbeiten scharenweise Ingenieure an dieser Technologie, darunter Schwergewichte wie Sony, Samsung und Apple. Es gibt keinen konkreten Zeitplan für die Technologie, aber rechnen Sie damit, dass sie eher früher als später auf den Markt kommt.

17.5.2 High Dynamic Range

Das menschliche Auge kann eine erstaunliche Vielfalt von Farben, Luminanz (Helligkeit) und Kontrast wahrnehmen. An der Leistungsfähigkeit des menschlichen Sehens interessierte Wissenschaftler haben für diese Merkmale sogenannte *Farbartdiagramme* definiert, die besser unter dem Begriff *Farbräume* bekannt sind (Abbildung 17.67).

Computer können nur einen Bruchteil dessen darstellen, was Menschen wahrnehmen können, und verwenden dementsprechend eingeschränkte Farbräume. Geräteübergreifend übereinstimmende Farbräume ermöglichen eine gewisse Einheitlichkeit bei der Ausgabe von Farben. Für die IT-Branche sind verschiedene Standards definiert worden. Lange war sRGB der Standard für die Bildschirmdarstellung von Bildern.

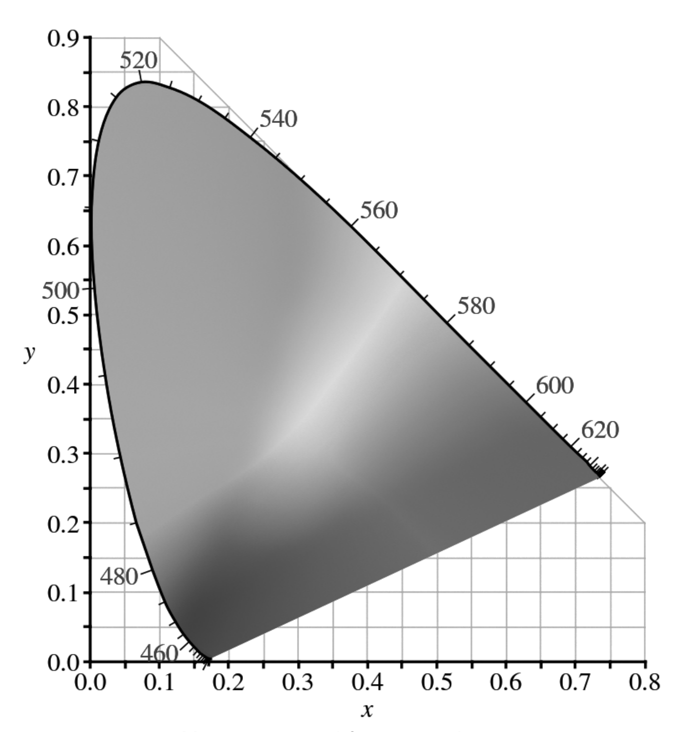


Abb. 17.67: Beispiel für einen Farbraum

Der Dynamikumfang (engl. *dynamic range*) eines Monitors spiegelt wider, wie viele Farbnuancen zwischen reinem Schwarz und reinem Weiß angezeigt werden können. Haben Sie schon einmal einen Sonnenaufgang oder Sonnenuntergang gesehen mit den phänomenalen Helligkeitsunterschieden zwischen den vom Sonnenlicht angestrahlten Wolken und den düsteren Schatten rund um Bäume? Das ist Dynamikumfang.

Ein normales 8-Bit-Panel verwendet SDR (*Standard Dynamic Range*), und das ist für die meisten Tätigkeiten am Computer (Filme, Spiele, Produktivanwendungen) ausreichend – bis man einen großen Monitor mit 10-Bit-Panel und HDR (*High Dynamic Range*) gesehen hat, bei dem es einem die Sprache verschlägt. Die sichtbaren Details, Texturen und Schattierungen sorgen für ein völlig anderes Erlebnis beim Betrachten der Computergrafik.

Hinweis

Ich wünschte, ich könnte Ihnen einen Vergleich von SDR und HDR zeigen, aber das ist in einem Buch nicht möglich. Besuchen Sie einen Computerladen und lassen Sie sich das vorführen.

17.5.3 Adaptive Sync

Wenn eine Grafikkarte ausgelastet ist, kann die Anzahl der pro Sekunde erzeugten Frames heftig schwanken. Sind Grafikkarte und Anzeige nicht synchron, kann es dazu kommen, dass verschiedene Bereiche des Bildschirms unterschiedliche Frames anzeigen. Dieser störende Effekt wird als *Tearing* (»Zerreißen« einzelner Bilder) bezeichnet, und die Hersteller von Grafikkarten und Bildschirmen beschäftigen sich seit Jahren mit diesem Problem.

Ein erster Lösungsansatz namens vertikale Synchronisierung (VSync) vermeidet Tearing durch eine fest vorgegebene Bildwiederholfrequenz (während des Bildaufbaus findet keine Aktualisierung der Bilddaten statt), allerdings auf Kosten einer höheren Latenz. *Adaptive Sync* nahm dieses Problem in Angriff, indem es dem Bildschirm ermöglichte, seine Bildwiederholfrequenz mit derjenigen der Grafikkarte zu synchronisieren. NVIDIA entwickelte eine proprietäre Adaptive-Sync-Technologie namens *G-Sync*. AMD reagierte darauf mit der Entwicklung einer lizenzfreien Adaptive-Sync-Technologie namens *FreeSync*. Von beiden Technologien gibt es mittlerweile eine zweite Generation mit HDR-Unterstützung: FreeSync 2 und G-Sync HDR.

Für Spiele bedeuten diese Technologien eine erhebliche Verbesserung, aber es gibt auch einen Nachteil: Die systemübergreifende Kompatibilität ist nur minimal. Um Adaptive Sync nutzen zu können, müssen sowohl Grafikkarte als auch Bildschirm entweder FreeSync oder aber G-Sync unterstützen. (Allerdings hat NVIDIA kürzlich angekündigt, eine Handvoll FreeSync-Monitore zu unterstützen.) Wenn Sie Adaptive Sync verwenden möchten, müssen Sie die Kompatibilität Ihrer Komponenten also sorgfältig überprüfen!

17.5.4 Grafikmodi

Ein Display mit der nativen Auflösung zu betreiben, ist wichtig, aber die Bildqualität wird in gewissem Maße auch davon abhängen, wie gut Grafikkarte, Betriebssystem, Anwendungen, Multimediadateien und Webseiten diese Auflösung unterstützen. Die Auflösungen werden auch als *Grafikmodi* oder *Anzeigemodi* bezeichnet, für die es jeweils eine eigene Abkürzung gibt.

All diese Auflösungen auswendig zu lernen, ist keine besonders sinnvolle Art und Weise, seine Zeit zu verbringen (es gibt wirklich *eine Menge* verschiedener Auflösungen), aber es ist sicherlich eine gute Idee, wenn Ihnen diejenigen vertraut sind, denen Sie in der Praxis begegnen werden oder zu denen man Ihnen Fragen stellt. In Tabelle 17.2 sind gebräuchliche Grafikmodi aufgeführt. Beachten Sie, dass hier keine mobilen Geräte berücksichtigt sind.

Grafikmodus	Auflösung	Seitenverhältnis	Typisches Gerät
VGA	640 x 480	4:3	Alte Monitore
SVGA	800 x 600	4:3	Alte Monitore
HDTV 720p	1.280 x 720	16:9	Kleinste Auflösung, die als HDTV bezeichnet wird
HDTV 1080p	1.920 x 1.200	16:9	Full-HDTV-Auflösung
WUXGA	1.920 x 1.200	16:10	Ältere Breitbildschirme
WQHD (2K)	2.560 x 1.440	16:9	Breitbildschirme
4K Ultra HD	3.840 x 2.160	16:9	Fernseher, sehr gute Monitore
5K	5.120 x 2.880	16:9	Sehr gute Monitore
8K Ultra HD	7.680 x 4.320	16:9	Fernseher

Tabelle 17.2: Verbreitete Anzeigemodi

17.5.5 eGPUs

Die Hersteller haben sich den rasend schnellen Datendurchsatz der neuesten USB-Version und von Thunderbolt zunutze gemacht, um externe GPUs zu entwickeln, eigenständige Geräte mit Grafikkarten zur Videobearbeitung oder zum Spielen. eGPUs ermöglichen es, unterwegs 4K-Videos zu bearbeiten und grafikintensive Spiele auf einem tragbaren Computer zu spielen, etwa auf Ultrabooks oder auf MacBook Pros. Die mobilen Geräte bleiben dünn und leicht, im Gegensatz zu den zum Spielen ausgelegten tragbaren Computern. Darüber hinaus brauchen Sie kein Geld für einen eigenen Rechner für

die Videobearbeitung oder zum Spielen auszugeben, wenn Sie einen leichten tragbaren Rechner benötigen.

Verschiedene Hersteller von Grafikkarten und Peripheriegeräten, wie Gigabyte, Alienware und ASUS, bieten unterschiedliche Varianten von eGPUs an. Die AORUS Gaming Box von Gigabyte wird mit einem Netzteil, einer hochwertigen NVIDIA-Grafikkarte, einer Hauptplatine und einem Gehäuse ausgeliefert, das zur Videoausgabe HDMI-, DP- und DVI- sowie vier USB-Anschlüsse besitzt. Die Verbindung zum tragbaren Computer wird über Thunderbolt hergestellt.

Der Graphics Amplifier von Alienware hingegen ist ein spezielles Gehäuse für Notebooks von Alienware. Eine Grafikkarte gehört nicht zum Lieferumfang, es gibt jedoch einen PCIe-Steckplatz, an den Sie eine GPU Ihrer Wahl anschließen können. Die Verbindung mit dem Computer erfolgt über einen speziellen Anschluss von Alienware. Die ROG XG Station 2 von ASUS bietet ähnliche Leistungsmerkmale wie das Modell von Alienware, kommt aber ohne proprietäre Verbindung aus.

Der Unterschied zwischen kompletten und selbst zusammengestellten Geräten spiegelt sich beim Preis wider. Das Gerät von Gigabyte kostet ca. 550 Euro, das von Alienware nur ca. knapp 200. ASUS ist vom Design des eigenen Gehäuses offenbar begeistert. Es wird für mehr als 450 Euro verkauft – ohne Grafikkarte!

17.6 Wiederholung

17.6.1 Fragen

1. Welcher Begriff beschreibt die Zeit, die es dauert, bis alle Subpixel eines LCD-Bildschirms von einem Zustand in einen anderen wechseln?
   A. Aktualisierungsrate
   B. Bildwiederholrate
   C. Reaktionszeit
   D. Bildwiederholfrequenz
2. Wodurch wird ein LCD-Bildschirm beleuchtet?
   A. Hintergrundbeleuchtung
   B. Inverter
   C. Lampe
   D. LCD-Panel
3. Dieter möchte an sein MacBook Pro einen LCD-Monitor mit DVI-Schnittstelle anschließen. Welche Art Adapter sollte er verwenden?
   A. BNC auf DVI
   B. DisplayPort auf HDMI
   C. Mini-HDMI auf VGA
   D. Thunderbolt auf DVI
4. Wie wird die Helligkeit eines Beamers angegeben?
   A. In Lumen
   B. In Pixeln
   C. In LEDs
   D. In CCFLs
5. Was bedeutet die Auflösung 1080p?
   A. 1.024 x 768
   B. 1.280 x 1.024

C. 1.680 x 1.050
D. 1.920 x 1.080

6. Wie nennt man den Prozessor einer Grafikkarte?
   A. CPU
   B. GPU
   C. GDDR
   D. MPU
7. Welche Microsoft-API unterstützt 3-D-Grafik?
   A. Active Desktop
   B. DirectX
   C. Glide
   D. OpenGL
8. Welche beiden Technologien werden als Hintergrundbeleuchtung von LCD-Monitoren eingesetzt?
   A. CCFL und LED
   B. CCFL und LCD
   C. CCFL und AC
   D. HDMI und DisplayPort
9. Ein Kunde beklagt sich telefonisch, dass der Projektor im Konferenzraum während einer Präsentation plötzlich ausgefallen ist. Was könnte die Ursache des Problems sein? (Wählen Sie zwei Antworten aus.)
   A. Der Netzanschluss hat sich gelockert.
   B. Die Projektorlampe ist durchgebrannt.
   C. Der Projektor ist in den Ruhezustand übergegangen, weil das Betriebssystem nicht dafür konfiguriert wurde, den Projektor als erweiterte Anzeige zu verwenden.
   D. Der Projektor hat sich überhitzt und sich ausgeschaltet, weil der Lüfter ausgefallen ist oder die Lüftungsschlitze verstopft sind.
10. Ein Kunde beschwert sich am Telefon darüber, dass sein LCD-Bildschirm flackert. Was ist höchstwahrscheinlich das Problem?
    A. Die Bildwiederholrate ist zu hoch.
    B. Die Bildwiederholrate ist zu niedrig.
    C. Die Kaltkathodenlampe (CCFL) für die Hintergrundbeleuchtung ist defekt.
    D. Die LED für die Hintergrundbeleuchtung ist defekt.

17.6.2 Antworten

1. **C.** Die Zeit, die es dauert, bis alle Subpixel eines LCD-Bildschirms von einem Zustand in einen anderen wechseln, heißt Reaktionszeit.
2. **A.** Dafür ist die Hintergrundbeleuchtung zuständig.
3. **D.** Dieter sollte einen Adapter von Thunderbolt auf DVI verwenden, um den LCD-Bildschirm an seinem MacBook Pro anzuschließen.
4. **A.** Die Helligkeit von Beamern wird in Lumen angegeben.
5. **D.** Die Auflösung 1080p entspricht 1.920 x 1.080.
6. **B.** Der Prozessor auf einer Grafikkarte wird als GPU bezeichnet.
7. **B.** Microsoft hat die DirectX-API entwickelt, um 3-D-Programme zu unterstützen.

8. **A.** LCD-Monitore verwenden zwei miteinander konkurrierende Technologien zur Hintergrundbeleuchtung: CCFL und LED.
9. **B, D.** Projektorlampen halten nur ein paar Tausend Stunden und können somit regelmäßig während einer Präsentation ausfallen. Wenn sich der Projektor wegen eines defekten Lüfters oder verstopfter Lüftungsschlitze überhitzt, schaltet er sich ab, um die Lampe zu schützen.
10. **C.** LCD-Monitore besitzen eine feste Bildwiederholrate, daher ist höchstwahrscheinlich die Kaltkathodenlampe (CCFL) defekt. LED-Hintergrundbeleuchtungen flackern nicht.

Netzwerk: Grundlagen | 18

Themen in diesem Kapitel:

- Sinn und Zweck des Netzwerks, Geräte und Anschlussmöglichkeiten
- Netzwerktechnologien und Ethernet
- Typische Implementierung eines Ethernet-Netzwerks

Heutzutage findet sich kaum noch ein Computer, der *nicht* mit einem Netzwerk verbunden ist. Ob es sich dabei um ein System handelt, das Teil eines großen Firmennetzwerks ist, oder um das Smartphone in Ihrer Jackentasche, jeder Computer verfügt über eine wie auch immer geartete Netzwerkverbindung. Dementsprechend hat die CompTIA den A+-Zertifizierungsprüfungen eine ganze Menge Stoff zu diesem Thema hinzugefügt.

Dieses Kapitel stellt Netzwerke ausführlich vor, insbesondere die dafür erforderliche Hardware und die Technologien, die in den heutzutage überall vorhandenen Netzwerken zum Einsatz kommen. Zunächst untersuche ich, welche Aufgaben Computer in Netzwerken übernehmen, damit Ihnen klar ist, welche Geräte und Dienste, die Sie zweifelsohne schon viele Male genutzt haben, hier eine Rolle spielen. Danach konzentriere ich mich im Hauptteil dieses Kapitels auf die inzwischen zum Standard gewordenen betriebssystemunabhängigen Netzwerktechnologien, die fast überall zum Einsatz kommen. Abschließend befasse ich mich mit den an normalen Arbeitsplätzen in der Praxis verfügbaren Technologien.

1002

18.1 Aufgaben vernetzter Computer

Denken Sie einen Moment darüber nach, wofür genau Sie Netzwerke benutzen. Die meisten Leute antworten, wenn man sie danach fragt: »Im Internet surfen« oder »YouTube-Videos ansehen« oder vielleicht auch »Um auf dem Drucker nebenan zu drucken.« Alles gute Gründe, um ein Netzwerk zu verwenden, aber was ist ihnen gemeinsam? In jedem der Beispiele verwenden Sie Ihren Computer (den lokalen Computer), um auf irgendwelche Dinge zuzugreifen, die sich auf dem entfernten Computer (und eben nicht auf Ihrem lokalen Computer) befinden. Was also macht entfernte Computer so interessant (Abbildung 18.1)?

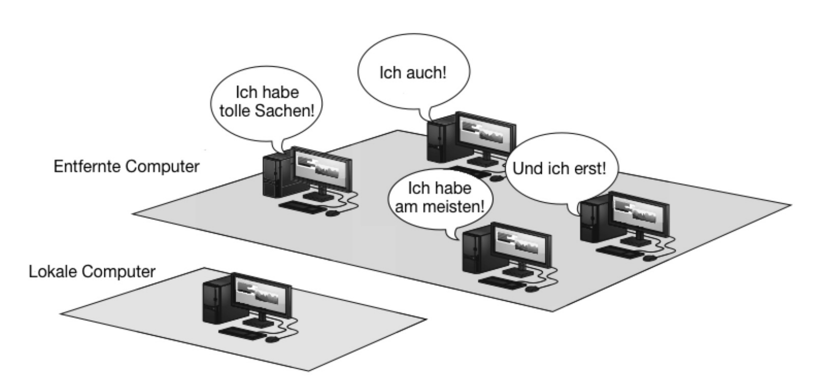


Abb. 18.1: Zugriff auf entfernte Computer

Hinweis

Bei vernetzten Computern kommen neue Begrifflichkeiten ins Spiel. Da die verschiedensten Geräte mit einem Netzwerk verbunden sein können, nicht nur PCs oder Macs, wird ein Begriff für vernetzte Geräte benötigt. Ein mit dem Netzwerk verbundenes Gerät wird als *Host* bezeichnet. Mit dem *lokalen Host* ist also das Gerät gemeint, vor dem Sie sitzen oder das Sie in Händen halten, wie z.B. Ihr Arbeitsplatzrechner. Ein *entfernter Host* hingegen ist ein anderes Gerät, das mit demselben Netzwerk verbunden oder auf andere Weise erreichbar ist (mehr dazu in Kürze).

Jeder Host im Netzwerk erfüllt eine bestimmte Aufgabe. Auf einem entfernten Computer, der als *Webserver* bezeichnet wird, sind die Dateien gespeichert, aus der eine Website besteht. Auf dem Webserver laufen Serverprogramme, die für die Speicherung und Auslieferung der Daten sorgen. Die beiden bekanntesten Webserver sind der Apache und IIS (Internet Information Server). Wenn Sie auf eine Website zugreifen, bittet Ihr Webbrowser (sehr wahrscheinlich Mozilla Firefox, Internet Explorer, Google Chrome oder Microsoft Edge) den Webserver, die Dateien der Webseite auszuliefern und stellt diese dann dar (Abbildung 18.2). Da die Anfrage von Ihrem Webbrowser ausgeht, wird er als *Client* bezeichnet. Den entfernten Computer, der die Inhalte »serviert«, nennt man *Server*.

Hinweis

Jeder Computer, auf dem ein Programm läuft, das Daten oder Dienste bereitstellt, ist per definitionem ein Server.

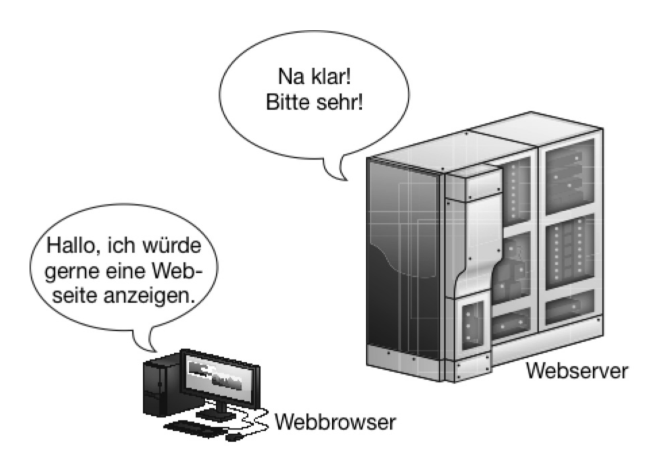


Abb. 18.2: Zugriff auf eine Webseite

Und was ist mit YouTube? Auch YouTube nutzt Webserver, die mit gigantischen Videodatenbanken verbunden sind. Diese entfernten Computer stellen, auf ähnliche Weise wie andere Webserver, Ihrem Client-PC Videos zur Verfügung, setzen dafür aber spezielle Software ein, die es ermöglicht, die Videodaten so schnell zu übermitteln, dass Sie Filme betrachten können, ohne darauf warten zu müssen (Abbildung 18.3).

Man braucht aber nicht unbedingt das Internet, um Dinge gemeinsam zu nutzen. In Abbildung 18.4 sehen Sie ein kleines Heimnetzwerk mit Computern, auf denen Windows läuft. Einer der Rechner im Netzwerk ist über den USB-Anschluss mit einem Drucker verbunden. Auf diesem Computer ist eine in Windows enthaltene Software zur Druckerfreigabe aktiv, sodass die anderen Rechner im Netzwerk den Drucker ebenfalls verwenden können. Dieser Computer nimmt also die Aufgabe eines *Druckerservers* wahr.

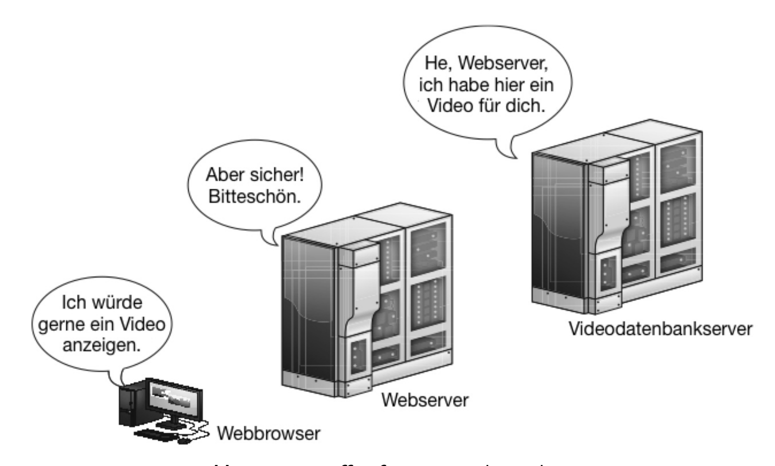


Abb. 18.3: Zugriff auf eine YouTube-Webseite

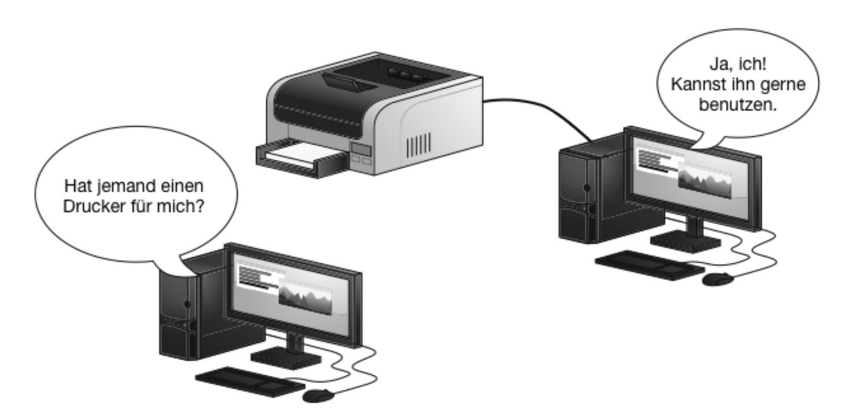


Abb. 18.4: Druckerfreigabe in Windows

Es spielt keine Rolle, wie groß das Netzwerk ist, wir verwenden es, um Dinge miteinander zu teilen. Dabei kann es sich um Webseiten, Videos, Drucker, E-Mails oder Musik handeln. Was Sie mit anderen teilen, wird nur dadurch beschränkt, dass Sie eine Serversoftware benötigen, die Objekte Ihrer Wahl bereitstellt und eine Clientsoftware, die darauf zugreifen kann.

Jede Art Server erhält eine Bezeichnung, die beschreibt, welche Aufgaben er wahrnimmt. Ein vernetzter Host, der den Zugang zu Dateien ermöglicht, heißt daher *Dateiserver*. Dementsprechend wird der vernetzte Host, den Sie zum Zugriff auf Ihre E-Mails nutzen, *Mailserver* genannt.

Hinweis

Neben vielen modernen Systemen gibt es auch eine Vielzahl älterer Systeme, die sehr spezielle Aufgaben erledigen. Der Hersteller eines Geräts könnte beispielsweise eine proprietäre Steuerung des Geräts über das Netzwerk einsetzen. Auch wenn es vielleicht technisch veraltet ist, braucht man das System nicht zu ersetzen, wenn es funktioniert.

Netzwerkfachleute bezeichnen alles, was ein Computer anderen bereitstellt, als *Ressource*. Die Aufgabe eines Netzwerks ist es daher, Computer miteinander zu verbinden, um Ressourcen freizugeben oder auf andere gemeinsam genutzte Ressourcen zuzugreifen.

Damit ein Netzwerk Ressourcen teilen und darauf zugreifen kann, sind folgende Voraussetzungen erforderlich:

1. Eine Festlegung und Standardisierung von Gestalt und Funktionsweise von Kabeln, Netzwerkkarten sowie der Verbindung mehrerer Computer.
2. Eine Adressierungsmethode, die es Clients gestattet, Server zu finden und es Servern ermöglicht, Daten an Clients zu senden, unabhängig von der Größe des Netzwerks.
3. Eine Möglichkeit, Ressourcen zu teilen und auf geteilte Ressourcen zuzugreifen.

Sehen wir uns also die erste dieser Voraussetzungen etwas näher an und werfen einen Blick auf die aktuellen Industriestandards.

Geschichte und Konzepte

18.2 Netzwerktechnologien

Als die ersten Netzwerkentwickler gemeinsam nach Möglichkeiten zur Verbindung von zwei oder mehr Rechnern und die gemeinsame Nutzung von Daten und Peripheriegeräten suchten, mussten sie eine Menge Details festlegen, um auch nur die grundlegendsten Fragestellungen zu beantworten. Die erste große Frage lautete: *Wie*? Es lässt sich leicht sagen: »Nun ja, dann verbinden wir die Kisten eben mit einem Kabel!« Damit wissen wir aber nicht, wie das Kabel funktioniert und wie es an einem Computer angeschlossen wird. Einige der wichtigen Fragen lauten beispielsweise:

- Wie lassen sich die einzelnen Rechner identifizieren?
- Wenn zwei oder mehr Rechner gleichzeitig kommunizieren wollen, wie lässt sich gewährleisten, dass alle Kommunikationsvorgänge korrekt verarbeitet werden?
- Welche Art von Kabel und welche Kabelmaße sollen verwendet werden? Wie viele Adern soll das Kabel enthalten? Welche Adern bzw. Leitungen sind für welche Aufgaben zuständig? Wie lang darf das Kabel maximal sein? Welche Anschlüsse sollen verwendet werden?

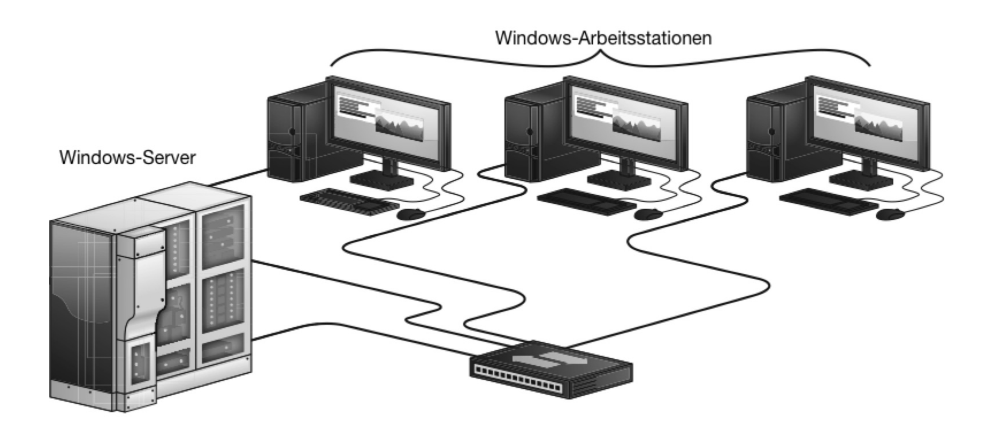


Abb. 18.5: Der Aufbau eines typischen Netzwerks

Um ein modernes PC-Netzwerk einzurichten, genügt es natürlich nicht, nur ein paar Kabel zu verlegen! Meist gibt es einen Client-Rechner, der Daten oder Dienste anfordert und einen Server, der diese bereitstellt. Sowohl der Client als auch der Server benötigen einen *Netzwerkadapter* (*NIC – Network*

Interface Card), der einen Rechner im Netzwerk definiert oder kennzeichnet. Netzwerkkarten sorgen auch dafür, dass Dateien für den Versand über das Netzwerk in kleinere Einheiten, sogenannte *Frames*, aufgeteilt werden und dass die empfangenen Datenpakete wieder zu kompletten Dateien zusammengesetzt werden. Weiterhin wird irgendein Medium als Übertragungsweg zwischen den verschiedenen Rechnern benötigt. Dabei handelt es sich zumeist um ein Kabel, das elektrische Signale transportiert. Oft werden aber auch Funkwellen oder andere drahtlose Verfahren genutzt. Und schließlich muss das Betriebssystem des Rechners mit seiner eigenen Netzwerkhardware und mit anderen Rechnern im Netzwerk kommunizieren können. Abbildung 18.5 zeigt ein Beispiel für den Aufbau eines typischen Netzwerks.

Wichtig

Bis vor einigen Jahren war eine NIC (Network Interface Card) tatsächlich eine Erweiterungskarte, die in einen Steckplatz auf dem Mainboard eingebaut wurde. Heutzutage ist die Netzwerkfähigkeit in praktisch allen Mainboards integriert und das Akronym NIC steht jetzt für Network Interface *Controller*. Ich verwende weiterhin auch den Begriff Netzwerkkarte.

1001

18.2.1 Frames und Netzwerkadapter

Daten werden in einzelnen Blöcken, die *Frames* (»Rahmen«) genannt werden, von einem Rechner zum anderen übertragen.

Hinweis

Oft hört man statt Frame den Begriff »Paket« – das ist aber nicht korrekt. Pakete sind genau genommen Bestandteile der Frames. In Kapitel 19 erfahren Sie mehr über Pakete.

Alle Netzwerkkarten besitzen eine eindeutige Kennung, die *MAC-Adresse* (*Media Access Control*) genannt wird. Bei der MAC-Adresse handelt es sich um eine Binärzahl, also um eine Aneinanderreihung von Nullen und Einsen. Jede Null oder Eins stellt ein Bit dar.

Die MAC-Adresse ist 48 Bit lang, sodass es insgesamt mehr als 281 *Billionen* MAC-Adressen gibt. Es stehen also immer noch eine Menge unbenutzter MAC-Adressen zur Verfügung. Da es Menschen sehr schwerfällt, sich so viele Nullen und Einsen zu merken, wird zur Anzeige dieser Adresse eine andere Methode verwendet. Durch *Hexadezimalzahlen* lassen sich Reihen von Nullen und Einsen in Kurzform darstellen. Hier ist eine Liste:

0000 = 0	0100 = 4	1000 = 8	1100 = C
0001 = 1	0101 = 5	1001 = 9	1101 = D
0010 = 2	0110 = 6	1010 = A	1110 = E
0011 = 3	0111 = 7	1011 = B	1111 = F

Die MAC-Adressen sind zwar eigentlich binär, werden aber üblicherweise als zwölf Hexadezimalzeichen angegeben. Diese MAC-Adressen sind fest in die Hardware der Netzwerkadapter eingebrannt und werden von vielen Herstellern auf einem Aufkleber auf dem Adapter selbst und oft auch auf der Verpackung angegeben. Natürlich lässt sich die MAC-Adresse aber auch mit Programmen auslesen. Abbildung 18.6 zeigt im Dienstprogramm SYSTEMINFORMATIONEN (`msinfo32`) die Beschreibung eines Netzwerkadapters, in der die MAC-Adresse markiert ist.

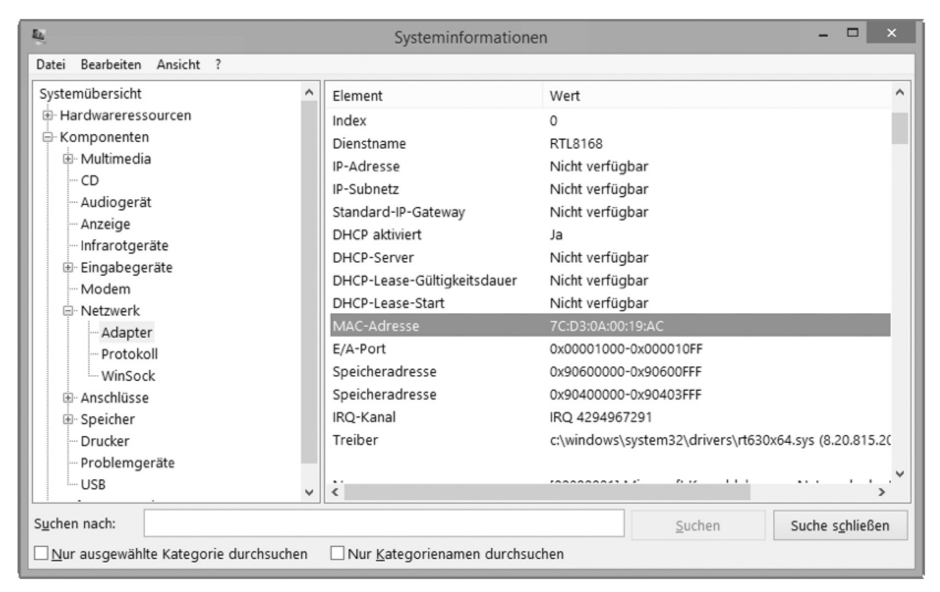


Abb. 18.6: MAC-Adresse

Hinweis

Auch wenn die MAC-Adresse fest in die Netzwerkkarte integriert ist, kann sie bei einigen NICs geändert werden. Dies ist jedoch nur selten erforderlich.

Aber geht es hier nicht um Frames? Schon, aber Sie müssen MAC-Adressen kennen, um Frames verstehen zu können.

Alle Varianten von Frames verfügen über bestimmte gemeinsame Merkmale (Abbildung 18.7). Erstens enthalten die Frames die MAC-Adresse der Netzwerkkarte, für die die Daten bestimmt sind. Zweitens enthalten sie die MAC-Adresse der Netzwerkkarte, von der aus die Daten gesendet werden. Drittens enthalten die Frames die Daten selbst (momentan wissen wir nicht, um welche Daten es sich handelt, da dafür bestimmte Software zuständig ist), deren Menge von der Art des verwendeten Frames abhängt. Schließlich müssen die im Frame enthaltenen Daten irgendwie geprüft werden, damit der empfangende Netzwerkadapter weiß, dass sie in ordnungsgemäßem Zustand empfangen wurden und in der richtigen Reihenfolge vorliegen. Die meisten Frames verwenden dazu einen pfiffigen mathematischen Algorithmus, der beim sogenannten *CRC*-Verfahren (*Cyclic Redundancy Check*) zum Einsatz kommt.

Tipp: Anzeige der MAC-Adresse

Einem Gerät wird für jede Netzwerkverbindung eine MAC-Adresse zugeordnet. Bei der Fehlersuche werden Sie des Öfteren die MAC-Adresse benötigen, probieren Sie also Folgendes aus!

In Windows, macOS und Linux gibt es mehrere Möglichkeiten, die MAC-Adresse herauszufinden. Am einfachsten gelingt das über die Kommandozeile. Geben Sie unter Windows in der Eingabeaufforderung `ipconfig /all` ein und drücken Sie ↵. Die MAC-Adresse wird als »Physische Adresse« im Abschnitt `Ethernet-Adapter` angegeben.

Was glauben Sie, welchen Befehl man in macOS und Linux dazu verwendet? Wie findet man heraus, welche Parameter übergeben werden müssen? Frischen Sie Ihre Kenntnisse auf und lesen Sie in Kapitel 15 nach!

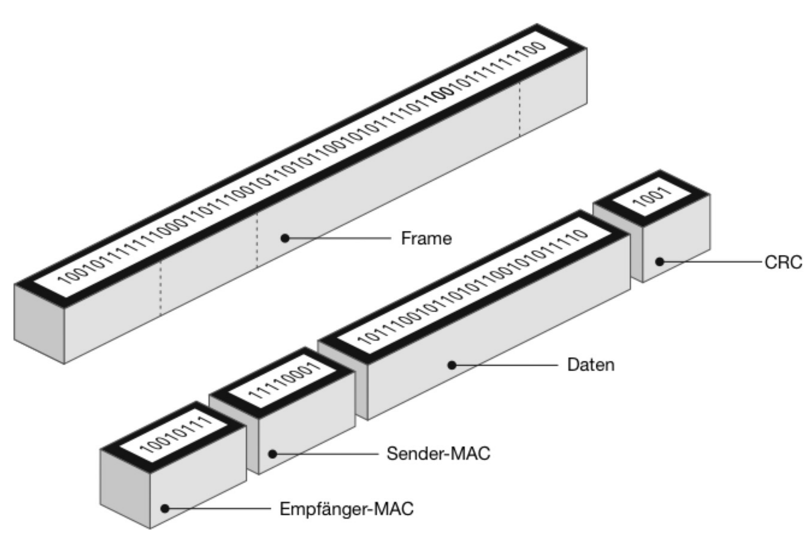


Abb. 18.7: Aufbau eines Frames

Bei dieser Beschreibung von Frames stellt sich die Frage, wie groß die Frames eigentlich sind, bzw. etwas spezifischer, wie viele Daten zu einem einzelnen Frame gehören. Wie lässt sich dafür sorgen, dass der empfangende Rechner versteht, *wie* die Daten vom sendenden Rechner aufgeteilt wurden und wie diese Teile wieder zusammengesetzt werden können? Die Antwort ist ein wenig problematisch, weil so viele verschiedene Aspekte einfließen. Als die ersten Netzwerke aufgebaut wurden, musste *alles* von den Frames über die Anschlüsse bis hin zum Kabel komplett neu erfunden werden.

Damit Netzwerke funktionieren können, müssen die sendenden und empfangenden Rechner dieselbe Netzwerktechnologie verwenden. Im Lauf der Jahre kamen und gingen verschiedene *Hardwareprotokolle*, aber eins dominiert heute die moderne PC-Landschaft deutlich: Ethernet. Ethernet wurde ursprünglich für kabelgebundene Netzwerke entwickelt, aber auch drahtlose Netzwerke verwenden Ethernet als Grundlage zur Erzeugung der Signale. Wenn Sie Netzwerke verstehen möchten, kommen Sie an Ethernet nicht vorbei.

18.2.2 Ethernet

Ein Firmenkonsortium um Digital Equipment, Intel und Xerox erfand Mitte der 1970er-Jahre das erste Netzwerk. Sie entwickelten aber nicht nur ein Netzwerk, sondern verfassten auch eine Reihe von Standards, in denen alle Einzelheiten definiert wurden, die für die Datenübertragung von einem Rechner zum anderen erforderlich waren. Diese Standards wurden *Ethernet* genannt. Im Laufe der Jahre wurden Hunderte von Verbesserungen eingeführt, die Bereich wie Geschwindigkeit, die Art der Signale oder den Kabeltyp betrafen.

Trotz all dieser Verbesserungen hat sich der Ethernet-Frame seit mehr als 25 Jahren nicht geändert. Das ist von entscheidender Bedeutung, denn da alle Ethernet-Varianten mit denselben Frames arbeiten, lassen sich Hardwarekomponenten und Verkabelungsvarianten in Ethernet-Netzwerken beliebig miteinander kombinieren. In den meisten Fällen können alle Rechner weiterhin problemlos miteinander kommunizieren.

Für die meisten modernen Ethernet-Netzwerke wird *10Base-T*, *100Base-T* oder *1000Base-T* als Technologie verwendet, oft auch bunt gemischt. Die Zahlen in den Bezeichnungen weisen auf die jeweils unterstützte maximale Datentransferrate hin: 10 Mbps bei 10Base-T, 100 Mbps bei 100Base-T (*Fast Ethernet*) und 1000 Mbps bzw. 1 Gbps bei 1000Base-T (*Gigabit-Ethernet*). Alle drei Technologien, die manchmal zusammenfassend 10/100/1000Base-T oder auch einfach nur Ethernet genannt werden, arbeiten mit einer *Stern-Bus-Topologie* und werden über *UTP-Kabel* (*Unshielded Twisted Pair*) verbunden.

Hinweis

Die Entwicklung von Ethernet steht natürlich nicht still. Es gibt noch immer Fast Ethernet (100BaseT) bei älteren Geräten. Gigabit Ethernet (1000Base-T) ist derzeit wohl der am weitesten verbreitete Standard, aber zwischen Servern sind bereits 10-Gigabit-Ethernet-Verbindungen üblich und 40/100-Gigabit-Ethernet etabliert sich auch allmählich.

Stern-Bus-Topologie

In allen Ethernet-Netzwerken werden die einzelnen Hosts per Kabel mit speziellen Anschlüssen an einem zentralen Kästchen verbunden. Das Kästchen kümmert sich zudem um alle lästigen Details, die beachtet werden müssen, damit die Frames an den richtigen Rechner gesendet werden. Dieser Aufbau des Netzwerks, der einem Stern ähnelt, wird als *Stern-Bus-Topologie* bezeichnet (Abbildung 18.8). (Der Begriff »Bus« bezieht sich auf die interne Verdrahtung im Kästchen, der Begriff »Stern« hingegen auf die Verkabelung der Hosts mit dem Kästchen. Stern-Bus ist daher eine Hybrid-Topologie.)

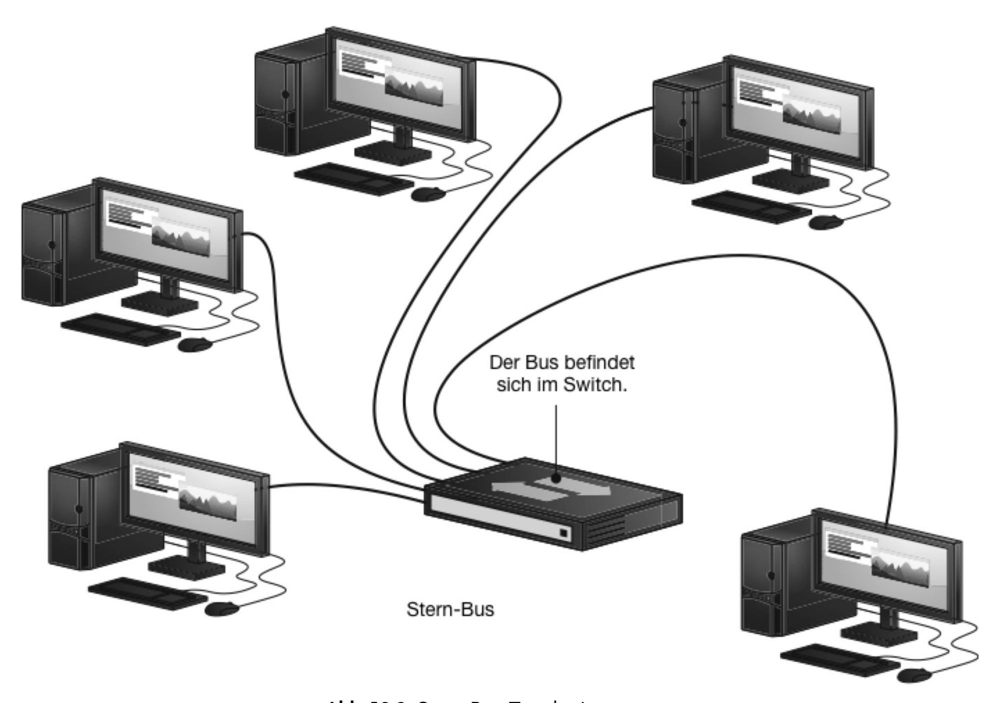


Abb. 18.8: Stern-Bus-Topologie

Das zentrale Kästchen mit dem Bus wird *Switch* genannt und stellt einen gemeinsamen Anschlusspunkt für Netzwerkgeräte bereit. Switches unterscheiden sich hinsichtlich der Anzahl der vorhandenen Anschlüsse. Die meisten einfachen Switches für Endverbraucher verfügen über vier bis acht Anschlüsse, während sie für den Einsatz in Unternehmen auch 32 oder mehr Anschlüsse besitzen können.

Die ersten Ethernet-Netzwerke setzten *Hubs* ein, ein *Switch* ist eine aktuellere und wesentlich leistungsfähigere Variante eines Hubs. Abbildung 18.9 zeigt einen typischen einfachen Switch.

Hubs und Switches sind äußerlich kaum zu unterscheiden und sie erledigen im Wesentlichen dieselbe Aufgabe: die Signale eines Hosts empfangen und sie an andere Hosts weiterzuleiten. Allerdings erfüllen Hubs und Switches diese Aufgabe auf ganz unterschiedliche Art und Weise. Ein Hub leitet die auf einem Port empfangenen Signale automatisch an alle anderen Ports weiter. Ein Switch hingegen spei-

chert die MAC-Adressen der angeschlossenen Geräte und leitet die empfangenen Signale nur an den jeweiligen Empfänger weiter. Geswitchte Netzwerke sind aus diesem Grund sehr viel schneller als über Hubs verkabelte.



Abb. 18.9: Ein Switch

Ein einfaches Beispiel soll den Unterschied zwischen Hubs und Switches illustrieren. Wenn Sie 32 Rechner mit einem 100-Mbps-Hub mit 32 Anschlüssen verbinden, dann müssen sich diese 32 Rechner die 100-Mbps-Bandbreite teilen. Ein Switch kann dieses Problem dadurch beheben, dass er im Prinzip aus jedem Anschluss ein separates Ethernet-Netzwerk macht. Allen Rechnern steht dann die gesamte Bandbreite zur Verfügung. Und das Fazit? Nachdem Switches bezahlbar wurden, sind Hubs schnell von der Bildfläche verschwunden.

Die Verbindung zwischen dem Switch und einem anderen Netzwerkgerät wird als *Segment* bezeichnet. Bei den meisten Kabeltypen darf die Länge eines Segments nicht mehr als 100 Meter betragen. Bei der Stern-Bus-Topologie ist es nicht möglich, ein Segment mittels eines Splitters in zwei oder mehr kleinere Segmente aufzuteilen, weil dadurch verhindert wird, dass der Switch erkennen kann, welcher Host Signale sendet oder empfängt. Ein an solch einem Segment angeschlossener Host könnte nicht kommunizieren. Darüber hinaus wirken sich Splitter negativ auf die Signalqualität aus.

Preiswert und zentralisiert fallen Stern-Bus-Netzwerke nicht gleich komplett aus, wenn einzelne Kabel defekt sind. Natürlich fällt das Netzwerk aus, wenn der Switch selbst defekt ist, aber das ist nur sehr selten der Fall.

UTP (Unshielded Twisted Pair)

10/100/1000Base-T arbeitet mit der UTP-Verkabelung, bei der es sich auch um die heute vorwiegend eingesetzte Verkabelungsvariante handelt. Es stehen viele TP-Kabelvarianten zur Auswahl, die je nach Anforderungen des Netzwerks eingesetzt werden können. TP-Kabel enthalten Leiter der Stärken AWG 22 bis AWG 26 (American Wire Gauge), die in farbcodierten Leitungspaaren paarweise verdrillt werden. Diese Leitungspaare werden dann locker von einem gemeinsamen, isolierenden Mantel umgeben.

Kabelkategorien (CATs) UTP-Kabel sind in verschiedenen Kategorien erhältlich, die über die mit dem Kabel maximal mögliche Geschwindigkeit der Datenübertragung (maximale Bandbreite) Aufschluss geben. Die Hauptkategorien (CATs) finden Sie in Tabelle 18.1.

CAT1	Standard-Telefonleitung
CAT3	Für 10-Mbps-Netzwerke ausgelegt; eine Variante, die alle vier Leitungspaare verwendet, unterstützt 100-Mbps
CAT5	Für 100-Mbps-Netzwerke ausgelegt
CAT5e	Verbesserte Ausführung, die 1000-Mbps-Netzwerke unterstützt

Tabelle 18.1: Kabelkategorien

CAT6	1000-Mbps-Netzwerke (bis zu 100 Meter lange Segmente); 10-Gbps-Netzwerke (bis zu 55 Meter lange Segmente)
CAT6a	10-Gbps-Netzwerke (100 Meter lange Segmente)
CAT6e	Nicht standardisierte Bezeichnung, die einige Hersteller für Kabel der Kategorien CAT6 oder CAT6a verwenden.
CAT7	10-Gbps-Netzwerke (100 Meter lange Segmente); die Abschirmung einzelner Leitungspaare verringert das Übersprechen der Signale und dämpft das Rauschen. CAT7 ist *kein* TIA/EIA-Standard.

Tabelle 18.1: Kabelkategorien (Forts.)

Die Kategorie sollte deutlich auf dem Kabel angegeben sein (Abbildung 18.10). Die Kategorisierung erfolgt durch die TIA/EIA (*Telecommunication Industry Association/Electronics Industries Alliance*) und unterliegt der Spezifikation 568. Gegenwärtig werden für die meisten Installationen CAT5e-, CAT6 oder CAT6a-Kabel verwendet.



Abb. 18.10: Angabe der CAT-Kategorie auf einem UTP-Kabel

STP (Shielded Twisted Pair)

STP-Kabel (*Shielded Twisted Pair*) besteht, wie der Name bereits andeutet, aus paarweise verdrillten Leitungen, die von einer Abschirmung umgeben sind, um sie vor elektromagnetischen Interferenzen (EMI) zu schützen. STP wird kaum eingesetzt, wahrscheinlich vorwiegend deshalb, weil die zusätzliche Abschirmung nur selten benötigt wird, denn diese spielt nur in Umgebungen eine Rolle, in denen starkes elektronisches Rauschen auftritt, wie z.B. in einem Ladengeschäft mit vielen Lampen, Elektromotoren oder anderen Geräten, die bei anderen Kabeln zu Einstreuungen und damit zu Problemen führen können.

18.2.3 Ethernet mit Twisted-Pair-Kabeln

Die 10/100 Base-T-Standards arbeiten mit zwei verdrillten Leitungspaaren, wobei über ein Paar Daten gesendet und über das andere Daten empfangen werden. 10Base-T funktioniert auch mit veralteten Kabeln der Kategorie CAT3, in der Praxis wird aber zumeist mindestens CAT5-Kabel eingesetzt. Für 100Base-T wird mindestens Kabel der Kategorie CAT5 benötigt, während für 1000Base-T, das alle vier Leitungspaare nutzt, mindestens CAT5e erforderlich ist. Diese Kabel verwenden einen speziellen Anschluss (einen sogenannten Westernstecker), der die Bezeichnung RJ-45 trägt. Die »RJ«-Kennung (*Registered Jack*) wurde vor Jahren vom amerikanischen Telefongiganten Bell geprägt und wird bis heute verwendet.

Hinweis

Eine Kategorisierung gibt es nicht nur für Kabel, sondern auch für Stecker. Versuchen Sie es besser gar nicht erst, einen CAT5e-RJ45-Stecker zusammen mit einem CAT6-Kabel zu verwenden.

Derzeit werden lediglich zwei Arten von RJ-Westernsteckern im Netzwerkbereich eingesetzt: RJ-11 und RJ-45 (Abbildung 18.11). RJ-11-Stecker dienen z.B. dem Anschluss des Telefonhörers an den Tele-

fonapparat. RJ-11 unterstützt zwei Leitungspaare, auch wenn die meisten Geräte nur zwei Leitungen benötigen. Die beiden anderen Leitungen können zur Unterstützung einer zweiten Telefonleitung genutzt werden. RJ-11-Anschlüsse werden vornehmlich für Internetverbindungen über die Telefonleitung genutzt (siehe Kapitel 21). RJ-45 ist der Standard für UTP-Anschlüsse. Der RJ-45-Westernstecker ist achtpolig und bietet damit Kontakte für maximal vier Leitungspaare und ist deutlich breiter als der RJ-11-Stecker. Abbildung 18.12 zeigt die Position der Pins 1 und 8 an einem RJ-45-Stecker.

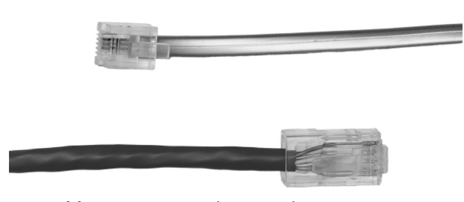


Abb. 18.11: RJ-11 (oben) und RJ-45 (unten)

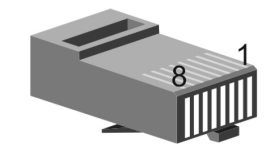


Abb. 18.12: Die Nummerierung der Kontakte eines RJ-45-Steckers

Es gibt zwei ANSI/TIA-Standards für den Anschluss von RJ-45-Steckern an UTP-Kabel: T568A und T568B. Beide sind verwendbar. Sie müssen sich an keinen bestimmten Standard halten, solange dieselben Leitungen am Ende des Kabels gepaart sind. Sie können sich das Leben jedoch ein wenig erleichtern, wenn Sie sich für einen der Standards entscheiden. Wenn alle Ihre Kabel demselben Standard entsprechen, können Sie sich letztlich eine Menge Arbeit sparen. Besonders wichtig ist aber, dass Sie sich Aufzeichnungen machen!

Wie bei allen Kabeln sind auch die Leitungen bei UTP nummeriert. Diese Nummern tauchen auf den Leitungen oder Anschlüssen allerdings normalerweise nicht auf. Die Leitungen sind aber farbig codiert. Die offiziellen Standard-Farbcodierungen der ANSI/TIA für UTP sind in Tabelle 18.2 aufgeführt.

Pin	568A	568B
1	Weiß/Grün	Weiß/Orange
2	Grün	Orange
3	Weiß/Orange	Weiß/Grün
4	Blau	Blau
5	Weiß/Blau	Weiß/Blau
6	Orange	Grün
7	Weiß/Braun	Weiß/Braun
8	Braun	Braun

Tabelle 18.2: Farbcodierung des UTP-Kabels

Tipp

Sehen Sie sich zur Prüfungsvorbereitung die »568B«-Simulation für Kapitel 18 an (`http://totalsem.com/100x`).

Plenum vs. PVC

Wenn Netzwerkkabel innerhalb von Gebäuden verlegt wird, dann werden diese meist hinter Verkleidungen oder innerhalb von Wänden so durch Kabelkanäle geführt, dass nur die Anschlusssteckdosen in den Wänden sichtbar sind. Der Raum unterhalb der Decke, unter den Fußböden und in den Wänden, durch den Kabel verlegt werden können, wird als *Plenum* bezeichnet. Problematisch daran ist jedoch, dass der Mantel bei Netzwerkkabeln aus Plastik besteht, das bei größerer Hitze Rauch und giftige Dämpfe erzeugt.

Standard-Netzwerkkabel haben normalerweise eine Ummantelung aus PVC (Polyvinylchlorid), aber PVC erzeugt bei einem Brand giftigen Rauch. Der Rauch, der durch brennende Kabel im Plenum entsteht, kann sich schnell über das gesamte Gebäude ausbreiten, deshalb sollten Sie im Plenum Kabel mit einem Feuer abweisenden Material verwenden. Plenum-fähige Kabel sind einfache Netzwerkkabel mit Feuer abweisendem Mantel, der für Kabel im Plenum-Bereich gefordert wird. Plenum-Kabel kostet das Drei- bis Fünffache wie PVC, aber Sie sollten es verwenden, wenn Sie Kabel im Plenum-Bereich verlegen.

18.2.4 Ethernet mit alternativen Kabelverbindungen

UTP-Kabel sind sehr beliebt, aber Ethernet kann, ebenso wie andere Netzwerkarten, auch andere Kabelverbindungen verwenden, die Sie kennen sollten. Jeder CompTIA A+-zertifizierte Techniker muss Glasfaser- und Koaxialkabel kennen.

Hinweis

Sie können zwei Computer direkt miteinander verbinden, wenn Sie ein sogenanntes *Crossover-Kabel* verwenden. Dabei handelt es sich um ein Standard-UTP-Kabel, dessen RJ-45-Stecker an einem Ende nach dem 568A-Standard und am anderen Ende gemäß 568B-Standard belegt sind. Dadurch sind die Leitungen zum Empfangen und Senden an einem Ende vertauscht, und das Kabel erledigt so die Aufgabe eines Hubs oder Switches. Crossover-Kabel sind bestens dazu geeignet, zwei PCs schnell miteinander zu verbinden. Sie erhalten die Kabel in jedem Computerladen.

Glasfaserkabel

Glasfaserkabel oder *Lichtwellenleiter* stellen eine äußerst attraktive Alternative zur Übertragung von Ethernet-Netzwerkpaketen dar. Erstens ist Glasfaserkabel gegenüber elektrischen Problemen (Blitzeinschlag, Kurzschluss und statische Elektrizität) immun, da es mit Licht und nicht mit Elektrizität arbeitet. Zweitens können Glasfasersegmente bei einigen Standards wesentlich länger werden (bis zu ca. 2000 m, während es bei der UTP-Verkabelung maximal 100 m sind). Das zumeist für Glasfaser-Ethernet verwendete Kabel wird »62.5/125 Multimode-Glasfaserkabel« genannt. Alle Glasfaser-Ethernet-Netzwerke erfordern zwei dieser Kabel. Abbildung 18.13 zeigt die drei am häufigsten in Glasfaser-Netzwerken verwendeten Stecker. Der runde Stecker links wird als *ST-Stecker* bezeichnet. Der quadratische Stecker in der Mitte heißt *SC-Stecker* und der ganz rechts wird *LC-Stecker* genannt.

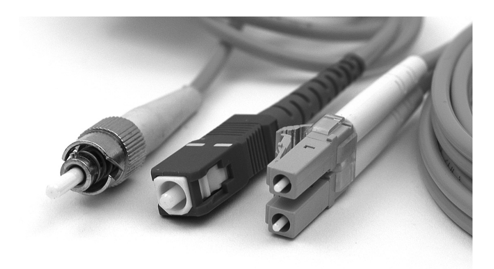


Abb. 18.13: Typische Glasfaserkabel mit Steckern

Wie viele andere Glasfaser-Anschlüsse arbeiten auch die älteren SC- und ST-Anschlüsse im Halbduplex-Modus, in dem die Daten nur in eine Richtung fließen, weshalb bei solchen Glasfaser-Installationen auch zwei Kabel benötigt werden. Neuere und hochwertigere Glasfaser-Installationen verwenden Anschlüsse mit Bezeichnungen wie LC, bei denen an einem Stecker zwei Kabel anschließbar sind, was viel Platz einspart.

Bei dem über Glasfaserkabel übertragenen Licht kann es sich um gewöhnliches Licht oder Laserlicht handeln. Dabei sind aber jeweils völlig andere Glasfaserkabel erforderlich. Bei den meisten Netzwerktechnologien, die mit Glasfaserkabel arbeiten, werden die zu übertragenden Lichtsignale mit LEDs erzeugt. Diese Netzwerke verwenden *Multimode*-Glasfaserkabel. Multimode-Glasfaserkabel kann mehrere Lichtsignale gleichzeitig übertragen, wenn diese unterschiedliche Reflexionswinkel im Kabelkern verwenden. Die verschiedenen Reflexionswinkel streuen aber über größere Distanzen, weshalb Multimode-Glasfaserkabel nur für relativ kurze Entfernungen geeignet ist.

Wichtig

Die verschiedenen Glasfaser-Anschlüsse und den Unterschied zwischen Multimode und Singlemode sollten Sie kennen.

Mit Laserlicht arbeitende Netzwerktechnologien verwenden Singlemode-Glasfaserkabel. Werden Laserlicht und Singlemode-Glasfaserkabel verwendet, lassen sich überaus hohe Datentransferraten über sehr große Entfernungen hinweg realisieren. Sieht man einmal von Fernverbindungen ab, wird Singlemode-Glasfaserkabel zurzeit noch selten verwendet, sodass Sie bei Begegnungen mit Glasfaserkabel ziemlich sicher sein können, dass es sich um Multimode-Kabel handelt.

Es gibt fast 100 verschiedene Glasfaserkabel-Standards, die Namen wie 1000BaseSX oder 10GBaseSR tragen. Der einzige wirkliche Unterschied besteht in der Geschwindigkeit des Netzwerks (es gibt auch noch einige wichtige Unterschiede hinsichtlich der Art, wie die Systeme untereinander verbunden werden usw.). Wenn Sie Glasfaserkabel verwenden möchten, benötigen Sie dafür geeignete Switches und Netzwerkkarten.

Beim Aufbau von Glasfasernetzwerken folgt man den Beschränkungen hinsichtlich Geschwindigkeit und Entfernung, die im jeweiligen Netzwerkstandard festgelegt sind, um keine bösen Überraschungen zu erleben. Daher ist es schwierig, für die tatsächlichen Grenzen genaue Zahlen zu nennen. Multimode ist insgesamt etwas langsamer und überbrückt geringere Distanzen als Singlemode. Typische Multimode-Netzwerke werden mit 10, 100 oder 1.000 Mbps betrieben, obwohl es auch welche mit 10.000 Mbps gibt. Die Kabellänge bei Multimode ist auf ungefähr 600 Meter beschränkt. Singlemode lässt Multimode hinsichtlich Geschwindigkeit und Distanz (je nach Standard) oft weit hinter sich. Die schon im Jahre 2011 erreichte Spitzengeschwindigkeit betrug beispielsweise 100 *Terabit* pro Sekunde bei einer Distanz von mehr als 160 *Kilometern*!

Wichtig

Es gibt verschiedene Ethernet-Standards, die Glasfaserkabel statt UTP-Kabel verwenden.

Koaxkabel/BNC-Kabel

Die ersten Ethernet-Netzwerke wurden statt mit UTP-Kabel über *Koaxialkabel* (kurz: Koaxkabel) verbunden. Die Ethernet-Standards verwenden schon lange keine Koaxkabel mehr, sie sind aber heute noch in Gebrauch, vor allem zum Anschluss von Kabelmodems oder Satellitenschüsseln. Bei Koaxkabel handelt es sich um eine von einer Isolation umgebene zentrale Ader (die das eigentliche Signal weiterleitet), um die herum sich wiederum eine Abschirmung aus verflochtenem Draht windet (Abbildung 18.14). Das gesamte Kabel ist dann wiederum von einem isolierenden Schutzmantel umgeben.



Abb. 18.14: Koaxkabel

Koaxialkabel werden mit RG-Kennungen bezeichnet. »RG« steht abkürzend für »Radio Grade«, einen Industriestandard für die technischen Daten von Koaxialkabel. Sie müssen von den vielen Standards nur zwei kennen: RG-59 (einfach geschirmt) und RG-6 (doppelt geschirmt). Beide Standards legen die Impedanz des Koaxialkabels fest, die in Ohm (Ω) gemessen wird. Sowohl RG-6- als auch RG-59-Koaxkabel besitzen eine Impedanz von 75 Ω und werden vornehmlich für Kabelfernsehen und Antennenkabel verwendet. (Die *Impedanz* ist der effektive Widerstand eines Kabels, das ein elektrisches Signal per Wechselstrom weiterleitet.) RG-59 ist allerdings dünner und überträgt Daten nicht ganz so weit wie RG-6. Die RG-Kennung sollte auf dem Kabel deutlich angegeben sein.

Hinweis

Es gehört zwar nicht zu den Lernzielen, aber es ist zu erwarten, dass künftig häufiger eine verbesserte Variante von RG-6 Einsatz findet, ein vierfach abgeschirmtes Koaxialkabel, das RG6QS heißt. Die zusätzliche Abschirmung verringert Interferenzen und ermöglicht stärkere Signale und damit höhere Datenübertragungsraten. (Wenn Sie dabei an mehrere Signale für 4K-Fernseher denken, liegen Sie richtig.)

Bei Koaxkabeln finden hauptsächlich zwei Stecker Verwendung: BNC-Stecker mit Bajonettverschluss (Abbildung 18.15) und ein Stecker mit der unprätentiösen Bezeichnung »Typ F« (Abbildung 18.16), den Sie vielleicht von Satellitenempfängern kennen.



Abb. 18.15: BNC-Stecker



Abb. 18.16: F-Typ-Stecker

Hinweis

Die Abkürzung »BNC« bedeutet Verschiedenes, je nachdem, wen Sie fragen. Die häufigsten Interpretationen sind *Bayonet Neill-Concelman* oder *British Naval Connector*. Verwenden Sie einfach den Begriff »BNC«, dann wird man schon verstehen, was Sie meinen.

Mit Koaxialkabeln können Datenübertragungsraten von mehr als 100 Mbps erreicht werden. Die Verwendung von Splittern wirkt sich negativ auf die Signalqualität aus und verringert die mögliche Datenübertragungsrate.

18.3 Ethernet-Implementierung

Es spielt keine Rolle, ob UTP-Kabel oder Glasfaser verwendet wird: Ethernet wird als Stern-Bus-Topologie implementiert. Natürlich sieht man in der Realität keinen »Stern«, der so deutlich zutage tritt wie in Abbildung 18.8. Sehen wir uns also kurz eine gebräuchliche Ethernet-Implementierung an.

18.3.1 Ein typisches LAN

Bei einem lokalen Netzwerk (LAN) handelt es sich um eine Gruppe von Computern, die sich in physischer Nähe zueinander befinden. Die Geräte sind nicht mehr als vielleicht ein paar Hundert Meter voneinander entfernt. Ein LAN kann sich in einem einzelnen Raum, Stockwerk oder Gebäude befinden. Die Computer in einem LAN können einander (zumindest fast immer) »hören«, wenn einer davon einen Broadcast aussendet. Eine solche Gruppe von Computern, die über einen Switch (oder mehrere Switches) miteinander verbunden sind, wird als Broadcast-Domäne bezeichnet (Abbildung 18.17), was bedeutet, dass alle Netzknoten Broadcastframes von allen anderen Netzknoten empfangen können.



Abb. 18.17: Zwei Broadcast-Domänen – zwei getrennte LANs

Wichtig

Merken Sie sich für die CompTIA A+-Prüfung, dass ein LAN aus einer Gruppe miteinander verbundener Computer in physischer Nähe besteht. Merken Sie sich auch, dass ein LAN in fast allen Fällen einer Broadcast-Domäne entspricht.

Sie können ein LAN in einer SOHO-Umgebung (*Small Office/Home Office*) auf verschiedene Weise einrichten. Die heutzutage übliche Methode per WLAN verzichtet ganz auf eine Verkabelung. Mehr dazu in Kapitel 20, *Drahtlose Netzwerke*.

Eine weitere Methode besteht darin, die vorhandenen elektrischen Leitungen eines Gebäudes für die Datenübertragung zu benutzen. Diese Art der Verbindung wird kurz als *PowerLAN* (oder auch *Powerline*) bezeichnet und erfordert spezielle *Bridges*, die an der Steckdose angeschlossen werden (Abbildung 18.18).

Eine *Bridge* ist ein Gerät, das zwei Netzwerke, die unterschiedliche Transportmedien verwenden, miteinander verbindet. Bridges werden auch eingesetzt, um drahtlose oder Koax-Netzwerke mit UTP-Netzwerken zu verbinden.

In manchen Fällen ist PowerLAN eine geeignete Lösung. Die schnellsten PowerLAN-Varianten erreichen dank einer Reihe von Innovationen fast die Geschwindigkeit von Gigabit-Ethernet. Wenn Sie einen Computer an einem ungewöhnlichen Ort betreiben, an dem es kein WLAN gibt und der auch mit herkömmlicher Verkabelung nicht erreichbar ist, haben Sie mit PowerLAN vielleicht eine Lösung gefunden.

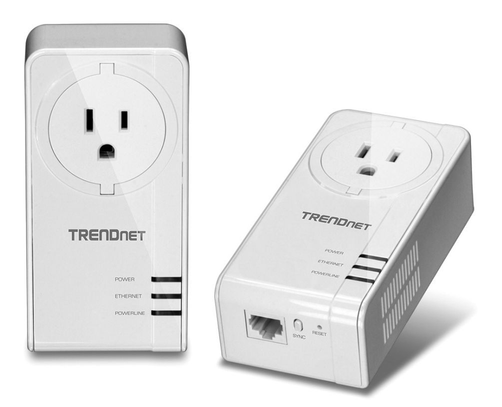


Abb. 18.18: PowerLAN-Adapter

18.3.2 Strukturierte Verkabelung

Zum reibungslosen und zuverlässigen Betrieb eines Netzwerks sind solide Kenntnisse verschiedener Standards erforderlich, die sich unter dem Begriff *strukturierte Verkabelung* zusammenfassen lassen. Diese Standards werden von der ANSI/TIA (*American National Standards Institute/Telecommunication Industry Association*) festgelegt. Genau, das sind die Leute, die auch die Pinbelegung am RJ-45-Stecker eines UTP-Kabels definiert haben. Professionelle Kabelinstallateure können sich bei allen Fragen der Netzwerkverkabelung nach diesen Standards richten, sei es nun der zu verwendende Kabeltyp, das Verlegen von Kabeln unter Putz oder die Position der Wandsteckdosen.

In den CompTIA A+-Prüfungen wird von Ihnen erwartet, dass Sie die betreffenden Konzepte der Netzwerkverkabelung verstanden haben und die verschiedenen Netzwerkkomponenten kennen. Sie müssen aber nicht über die Kenntnisse eines professionellen Kabelinstallateurs oder Netzwerkarchitekten verfügen. Ihr Ziel sollte es sein, genügend Wissen über echte Netzwerke zu erlangen, um fachmännisch mit Kabelinstallateuren kommunizieren und einfache Fehler selbst beheben zu können. Am Ende dieses Kapitels wissen Sie zwar mehr als genug, um Ihre Verkabelung selbst in die Hand zu nehmen (ich mache das jedenfalls), aber dennoch sollten Sie diese Kenntnisse nur als eine Art Bonus betrachten.

Grundsätzlich soll durch strukturierte Verkabelung eine sichere, zuverlässige Infrastruktur für alle verbundenen Geräte erzielt werden. Das betrifft selbstverständlich das Computernetzwerk, aber auch Telefone und Fernseher oder Videogeräte – alle Geräte, für deren Betrieb eine Verkabelung erforderlich ist.

Hinweis

Die strukturierte Verkabelung ist nicht nur in Computernetzwerken nützlich. Sie finden sie beispielsweise auch bei Telefonanlagen oder Videokonferenzsystemen.

Sie müssen drei Dinge über die strukturierte Verkabelung wissen. Zunächst sehen wir uns die Grundlagen der Verbindung von Switches und Computern an. Anschließend betrachten wir die Komponenten eines Netzwerks, etwa wie die Verkabelung verläuft und wo sie endet. Zum Abschluss beurteilen wir Verbindungen, die aus dem lokalen Netzwerk herausführen.

Grundlagen

Am Anfang dieses Kapitel haben wir uns mit einem Netzwerk in der einfachsten Form befasst: ein Switch, einige UTP-Kabel und ein paar PCs, also ein typisches Netzwerk mit Stern-Topologie (Abbildung 18.19).



Abb. 18.19: Ein Switch und zwei per UTP-Kabel angeschlossene PCs

Niemand kann Sie davon abhalten, einen Switch mitten in Ihrem Büro aufzustellen und die Kabel kreuz und quer durch die Räume zu verlegen, um sie an die PCs anzuschließen. Das funktioniert zwar, wird im wahren Leben aber grandios scheitern. Der Netzwerkfachmann sieht hier drei Probleme: Erstens warten die frei verlegten Kabel nur darauf, dass jemand darüber stolpert, der sich dann die Gelegenheit nicht entgehen lässt, Sie zu verklagen. Allein die ständigen Bewegungen und das Herumlaufen auf den Kabeln werden im Laufe der Zeit für deren Ausfall sorgen, da die Leitungen dadurch beschädigt werden oder die Steckverbindungen abbrechen können. Zweitens können andere elektrische Geräte in der Nähe der Kabel zu elektromagnetischen Interferenzen führen, was negative Auswirkungen auf die im Kabel transportierten Signale hat. Und drittens sind die Möglichkeiten, das Netzwerk zu ändern oder zu erweitern, sehr eingeschränkt. Bevor Sie etwas umstecken können, müssen Sie zunächst in dem ganzen Kabelsalat herausfinden, welches Kabel mit welchem Rechner oder Switch verbunden ist. Was für ein Albtraum!

»Meine Güte!«, werden Sie jetzt denken, »es muss doch eine bessere Methode geben, um ein physisches Netzwerk einzurichten.« Eine vernünftige Installation ist sicher und schützt die Stern-Topologie vor dem Staubsauger, ungeschickten Kollegen und elektromagnetischen Interferenzen. Es gibt darüber hinaus zusätzliche Hardware, um die Verkabelung zu schützen und zu organisieren. Schließlich verwendet eine ordentliche Stern-Topologie eine Verkabelungsmethode, die es erlaubt, das Netzwerk bei Bedarf flexibel zu erweitern oder auszubauen, sobald eine neue Netzwerktechnologie zum Standard wird. Das ist strukturierte Verkabelung!

Aufbau der strukturierten Netzwerkverkabelung

Die erfolgreiche Implementierung einer strukturierten Verkabelung setzt drei Dinge voraus: einen Telekommunikationsraum, horizontale Verkabelung und den Bereich zum Arbeiten. Lassen Sie uns ein typisches Büro betrachten. Sämtliche Kabel verlaufen von den einzelnen PCs zu einem zentralen Ort, dem *Telekommunikationsraum*. Welche Art von Geräten hier untergebracht ist, sei es ein Switch oder eine Telefonanlage, ist nicht entscheidend. Von Bedeutung ist, dass alle Kabel hier zusammenlaufen.

Sämtliche Kabel verlaufen vom Telekommunikationsraum zu den PCs (größtenteils) horizontal. Man bezeichnet das treffenderweise als *Horizontalverkabelung* der Leitungen. Am Ende der Leitung befindet sich der Arbeitsbereich, bei dem es sich oft um ein Büro oder eine Arbeitsnische mit Telefon und PC handelt. Abbildung 18.20 zeigt die Horizontalverkabelung und den Arbeitsbereich.

Bei jedem dieser drei Bestandteile einer Stern-Topologie (Telekommunikationsraum, Horizontalverkabelung und Arbeitsplatz), sind strenge Standards einzuhalten, die darauf abzielen, dass die Verkabelung zuverlässig ist und sich einfach verwalten lässt. Die von der ANSI/TIA festgelegten Standards ermöglichen es Technikern, sinnvolle Entscheidungen für die Geräte im Telekommunikationsraum zu fällen, daher befassen wir uns zunächst mit der Horizontalverkabelung, dann mit dem Telekommunikationsraum und schließlich mit dem Arbeitsplatz.

Horizontalverkabelung Die Horizontalverkabelung verläuft mehr oder weniger horizontal vom Arbeitsplatz zum Telekommunikationsraum. In den meisten Netzwerken kommen UTP-Kabel

(CAT5e oder besser) zum Einsatz. In den Standards spielen bei der strukturierten Verkabelung aber auch noch andere Aspekte eine Rolle, wie z.B. die Art der Drähte, die Anzahl der Adernpaare und Brandschutzbestimmungen.

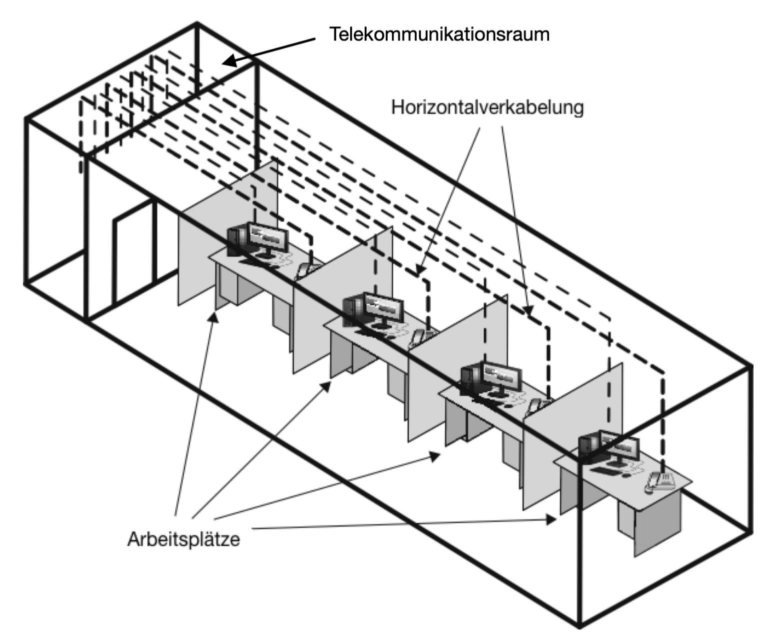


Abb. 18.20: Arbeitsplätze und Horizontalverkabelung

Einadrige und mehradrige Leitungen Es gibt zwei Arten von Leitungen bei UTP-Kabeln: einadrige oder mehradrige. Bei einadrigen Leitungen handelt es sich um einen einzigen, soliden Draht, während mehradrige Leitungen aus mehreren feinen Drähten bestehen (Litze). Vor- und Nachteile haben beide Typen. Einadrige Leitungen sind bessere Stromleiter, aber auch sehr starr und sie brechen, wenn sie zu oft oder zu ruppig bewegt werden. Mehradrige Leitungen leiten den Strom zwar weniger gut, vertragen aber eine beträchtliche Belastung, ohne zu brechen. Abbildung 18.21 zeigt eine Großaufnahme von einadrigem und mehradrigem UTP-Kabel.

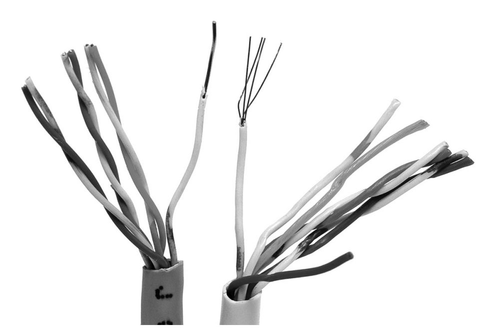


Abb. 18.21: Einadrige und mehradrige Leitungen von UTP-Kabeln

Gemäß TIA/EIA-Spezifizierung soll für die Horizontalverkabelung stets einadriges UTP-Kabel verwendet werden. Bedenken Sie hier, dass die Kabel hinter Wänden oder Verkleidungen verlegt werden und somit den schädigenden Effekten von Schuhen und Staubsaugern nicht ausgesetzt sind. Daher ist

es sinnvoll, die bessere Leitfähigkeit der einadrigen Leitungen zu nutzen, ohne Gefahr zu laufen, dass diese beschädigt werden. Auch mehradrige Leitungen haben bei der strukturierten Verkabelung ihr Einsatzgebiet, allerdings muss ich noch einige andere Netzwerkkomponenten erörtern, bevor ich darauf zurückkomme.

Der Telekommunikationsraum

Der Telekommunikationsraum ist das Kernstück der Stern-Topologie. Hier laufen sämtliche Leitungen von den Arbeitsplätzen zusammen. Durch die Anhäufung von Geräten im Telekommunikationsraum ist er ein Kandidat für den unordentlichsten Ort in der Stern-Topologie. Auch wenn Sie bei der Erstinstallation sorgfältige, ordentliche Arbeit geleistet haben, ändert das nichts daran, dass Netzwerke sich im Laufe der Zeit verändern. Die Leute ziehen mit den Rechnern um, neue Arbeitsplätze kommen hinzu, und manchmal werden sogar ganze Netzwerk-Topologien hinzugefügt oder ausgebaut. Wenn Sie hier keine Organisationsmaßnahmen treffen, kann diese Ansammlung von Geräten und Kabeln allmählich zu einem albtraumhaften Durcheinander verfallen.

Glücklicherweise sehen die TIA/EIA-Standards spezielle Komponenten für den Telekommunikationsraum vor, sodass die Organisation zum Kinderspiel wird. Man könnte sogar behaupten, dass es schon fast zu viele Optionen gibt! Wir betrachten daher nur die gebräuchlichste Einrichtung eines Telekommunikationsraums und werfen dann einen kurzen Blick auf einige der zusätzlichen, nicht so weit verbreiteten Möglichkeiten.

Geräte-Racks Zentraler Bestandteil des Telekommunikationsraums sind Geräte-Racks. Das *Geräte-Rack* bietet einen sicheren, stabilen Standort für die verschiedenen Hardware-Komponenten. Alle Geräte-Racks sind 19 Zoll (ca. 48 cm) breit, variieren in der Höhe aber von 60 bis 90 cm (wandmontierte Modelle, siehe Abbildung 18.22) bis zu den häufigeren, bis zur Decke reichenden Modellen (Abbildung 18.23).

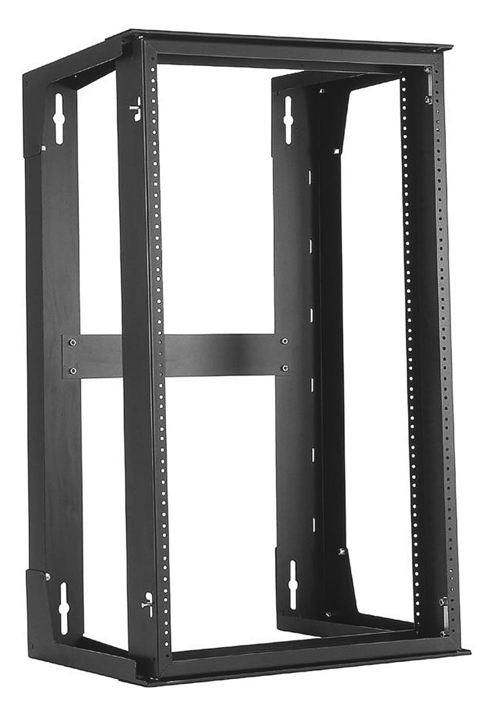


Abb. 18.22: Ein wandmontierbares Geräte-Rack



Abb. 18.23: Ein bis zur Decke reichendes Geräte-Rack

Hinweis

Geräte-Racks sind eine Weiterentwicklung von Signaltechnik-Anlagen der Eisenbahn des 19. Jahrhunderts. Natürlich haben die heutigen Komponenten in Geräte-Racks nichts mit Eisenbahn-Signaltechnik gemeinsam, aber das 19-Zoll-Maß hat sich seit weit mehr als 100 Jahren gehalten.

In ein Geräte-Rack können Sie so ziemlich jede für die Einrichtung eines Netzwerks erforderliche Hardware-Komponente einbauen. Sämtliche Hersteller bieten Switches an, die sich mit wenigen Schrauben in einem Rack montieren lassen. Solche Switches sind in vielerlei Form mit den verschiedensten Anschlüssen und Fähigkeiten verfügbar. Es gibt auch USV (Unterbrechungsfreie Stromversorgungen, Abbildung 18.24) und Server zum Einbau in Geräte-Racks, deren Tastatur sich wie eine Schublade herausziehen lässt.



Abb. 18.24: Rack-montierbare USV

Zur Beschreibung von Racks wird die *HE* (Höheneinheit) verwendet. Eine HE entspricht 1,75 Zoll bzw. 4,445 cm. Ein Gerät, das diese Höhe besitzt, wird als 1-HE-Gerät bezeichnet, eines, das die doppelte Höhe besitzt, als 2-HE-Gerät usw. Die meisten Geräte belegen 1, 2 oder 4 HE.

Patchfelder und Kabel Im Idealfall sollten Sie die Horizontalverkabelung nach der Erstinstallation nie wieder bewegen. Wie Sie wissen, werden einadrige Leitungen verwendet und diese sind ziemlich starr. Die eine oder andere Neuverlegung vertragen die Kabel schon, aber bei jedem Umstecken eines Kabelbündels oder beim Umpositionieren eines Switches machen Sie es etwas schlimmer. Allzu oft muss ein einadriges Kabel nicht neu verlegt werden, bis einer der starren Kupferdrähte bricht – und schon funktioniert die Netzwerkverbindung nicht mehr!

Glücklicherweise gibt es *Patchfelder*, mit deren Hilfe sich dieses Problem umgehen lässt. Dabei handelt es sich um einen Rahmen, in dem auf der Vorderseite Verbindungsbuchsen aufgereiht sind, die auf der Rückseite fest mit der Horizontalverkabelung verbunden sind (Abbildung 18.25).

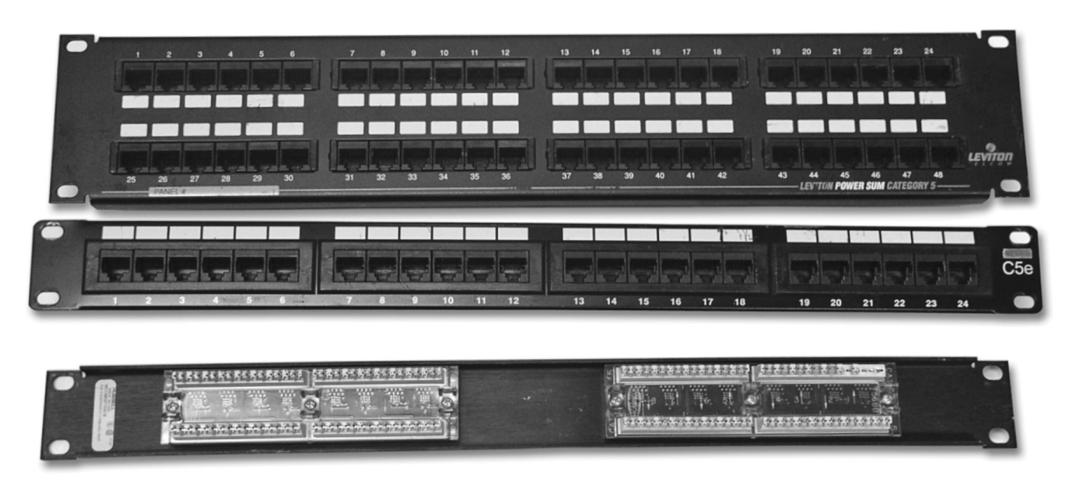


Abb. 18.25: Typische Patchfelder

Bei den heutzutage gebräuchlichsten Patchfeldern findet ein sogenannter *110-Block-Anschluss* Verwendung, an den mittels eines Punchdown-Tools das UTP-Kabel angeschlossen wird. Abbildung 18.26 zeigt ein typisches Punchdown-Tool und in Abbildung 18.27 können Sie sehen, wie es zum Befestigen der einzelnen Drähte verwendet wird.



Abb. 18.26: Punchdown-Tool

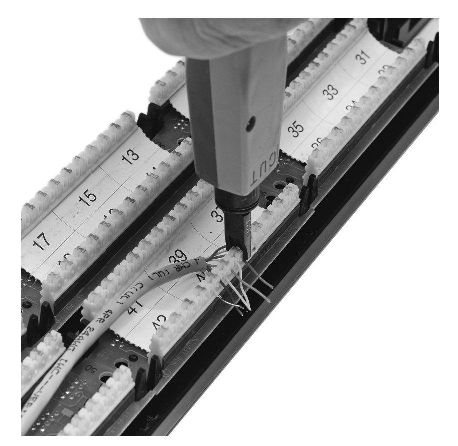


Abb. 18.27: Punchdown-Tool und 110-Block

Der 110-Block besitzt kleine Einkerbungen aus Metall für die einzelnen Drähte. Mit der stumpfen Zunge des Punchdown-Tools werden die Drähte in die Einkerbungen gepresst. Dabei schlitzt das Metall in den Einkerbungen die Ummantelung der Drähte auf und stellt so sicheren Kontakt her.

Wichtig

Sie sollten wissen, dass zum Herstellen einer sicheren Verbindung zwischen 110-Block und UTP-Kabel ein Punchdown-Tool verwendet wird. Wie genau das Werkzeug gebraucht wird, ist aber erst Thema der CompTIA Netzwerk+-Zertifizierung.

Durch Patchfelder wird nicht nur verhindert, dass die Horizontalverkabelung bewegt werden muss. Sie ermöglichen außerdem die Organisation der Verkabelung. Alle Anschlüsse eines Patchfelds bieten Platz zum Anbringen kleiner Etiketten und das ist für Techniker eine große Hilfe. Kleben Sie einfach so ein Schildchen neben den Anschluss, um ihn identifizieren zu können. Sie werden dann niemals das unerfreuliche Gefühl erleben müssen, dass einen im Telekommunikationsraum beschleicht, wenn das Netzwerk nicht funktioniert und man sich fragt, welches Kabel wohin gehört. Es gibt sogar eine offizielle, ziemlich verwirrende Kennzeichnungsmethode der ANSI/TIA namens ANSI/TIA 606, aber viele Netzwerktechniker verwenden lieber ein Verfahren nach eigenem Gutdünken (Abbildung 18.28).

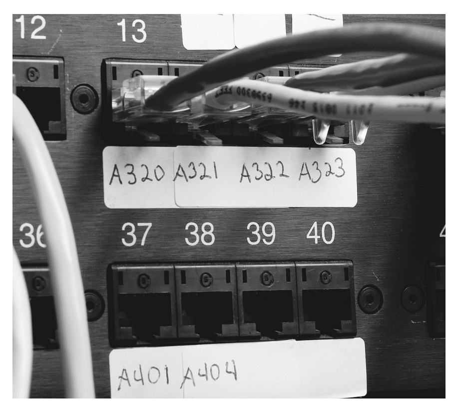


Abb. 18.28: Patchfeld mit Etiketten

Patchfelder gibt es in den verschiedensten Ausführungen, mit unterschiedlichen Anschlusstypen und variierender Zahl von Anschlüssen. Es sind Patchfelder mit UTP-, STP- oder Glasfaser-Anschlüssen erhältlich. Einige Hersteller bieten auch Patchfelder an, auf denen die verschiedenen Anschlüsse auf einem Patchfeld miteinander kombiniert sind. Es gibt Ausführungen mit 8, 12, 24, 48 oder sogar noch mehr Anschlüssen.

Ebenso wie bei UTP-Kabeln gibt es auch für UTP-Patchfelder eine Kategorisierung, die Sie unbedingt überprüfen sollten. Verderben Sie sich eine tolle CAT6-Verkabelung nicht durch ein billiges Patchfeld – besorgen Sie ein passendes CAT6-Patchfeld! Patchfelder der besseren Kategorien sind abwärtskompatibel, sodass es kein Problem ist, ein CAT6- oder vielleicht sogar CAT6a-Patchfeld mit einer CAT5e-Verkabelung zu verwenden. Bei vielen Herstellern ist die Kategorie an prominenter Stelle angegebenen (Abbildung 18.29).

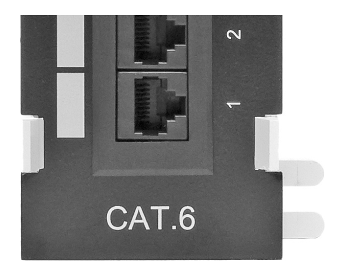


Abb. 18.29: Kategorieangabe eines Patchfelds

Nachdem das Patchfeld installiert ist, müssen Sie Buchsen mittels *Patchkabeln* mit dem Switch verbinden. Patchkabel sind relativ kurze (typischerweise ca. 50 bis 150 cm) UTP-Kabel (Abbildung 18.30). Die Leitungen sind mehradrig, damit die Kabel es besser überstehen, wenn sie gelegentlich umgesteckt werden. Es ist gar nicht schwer, Patchkabel selbst zu machen, aber die meisten Leute bevorzugen es, vorgefertigte zu kaufen. Wenn Sie verschiedenfarbige Patchkabel kaufen, können Sie sich die Organisation weiter vereinfachen: gelbe Kabel für die Buchhaltung, blaue Kabel für den Vertrieb, oder was auch immer Ihnen geeignet erscheint. Die meisten Patchkabel besitzen verstärkte Stecker, die dafür ausgelegt sind, möglichst viele Steckvorgänge zu überstehen.



Abb. 18.30: Typisches Patchkabel

Patchkabel selbst gemacht Die meisten Leute kaufen fertige Patchkabel, dabei ist es gar nicht so schwer, diese herzustellen. Verwenden Sie dazu mehradriges UTP-Kabel derselben Kategorie, die bei der Horizontalverkabelung eingesetzt wurde. Für mehradriges Kabel gibt es spezielle Crimps, benutzen Sie also keine Crimps für einadrige Kabel. *Crimpen* ist eigentlich gar nicht so schwer, es erfordert jedoch etwas Übung.

Abbildung 18.31 zeigt das wichtigste Werkzeug beim Crimpen: eine RJ-45-Crimpzange mit den Vorrichtungen zum Abisolieren und Durchtrennen der Drähte. Professionelle Kabelinstallateure benutzen natürlich noch eine Reihe weiterer Spezialwerkzeuge.



Abb. 18.31: Crimpzange

Wichtig

Sie sollten wissen, dass Kabelinstallateure eine Crimpzange verwenden, um RJ-45-Stecker am Ende eines UTP-Kabels anzuschließen.

Es folgt eine Kurzanleitung zum Ancrimpen eines RJ-45-Steckers an das Ende eines UTP-Kabels. Mehr als ein paar Crimps, Kabel und eine Crimpzange benötigen Sie dazu nicht!

1. Durchtrennen Sie das Kabel mit der Crimpzange oder einem Seitenschneider.
2. Entfernen Sie ca. 1,5 cm der Kunststoffummantelung am Ende des Kabels (Abbildung 18.32).
3. Positionieren Sie die einzelnen Drähte gemäß ANSI/TIA 568A oder B an der entsprechenden Stelle (Abbildung 18.33). Versuchen Sie, die Litze dabei möglichst nicht zu entwirren.
4. Legen Sie den Crimp in die Crimpzange und drücken Sie zu (Abbildung 18.34). Sie brauchen sich keine Sorgen zu machen, dass Sie die Zange vielleicht zu fest zusammendrücken, da die Zange eine Blockierung besitzt, die das verhindert.

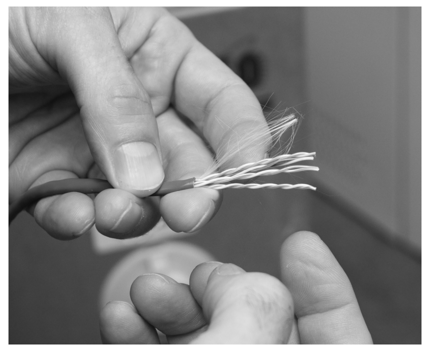


Abb. 18.32: Das abisolierte Kabel

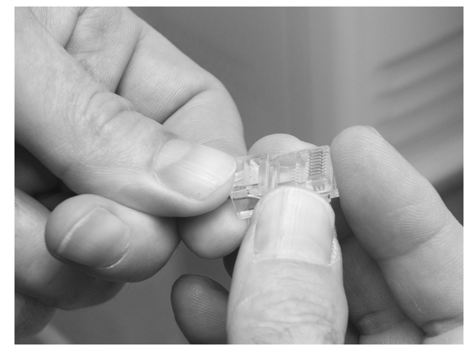


Abb. 18.33: Positionieren der einzelnen Drähte



Abb. 18.34: Zusammendrücken der Crimpzange

Abbildung 18.35 zeigt ein ordnungsgemäß gecrimptes Kabel. Beachten Sie, dass die Kunststoffummantelung bis in den Crimp hineinreicht. (Die zusätzlichen Fäden, die neben den eigentlichen Drähten erkennbar sind, werden als *Kennfäden* bezeichnet. Sie bestehen aus einem widerstandsfähigen Kunststoff (Kevlar) und verstärken das Kabel. Sie ermöglichen es dem Installateur, die Kabelummantelung leichter zu entfernen.)

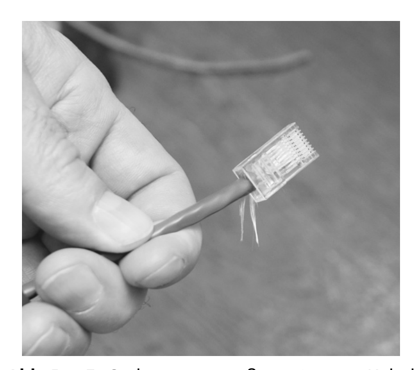


Abb. 18.35: Ordnungsgemäß gecrimptes Kabel

Bei einem ordentlichen Patchkabel gibt es auch eine Kappe. Abbildung 18.36 zeigt das Aufschieben der Kappe bei einem neuen Kabel. Denken Sie daran, die Kappen an beiden Enden des Kabels *vor* dem Crimpen aufzusetzen.



Abb. 18.36: Aufschieben der Kappe

Wenn das Kabel fertig ist, müssen Sie es ausprobieren, um sicherzustellen, dass Sie alles richtig gemacht haben. Ich verwende einen praktischen Kabeltester, erhältlich in jedem gut sortierten Elektronikfachgeschäft, um die einzelnen Drähte und deren Funktion zu überprüfen (Abbildung 18.37).



Abb. 18.37: Kabeltester

Der Arbeitsplatz

Beim Verkabeln ist der »Arbeitsplatz« einfach nur eine Wandsteckdose, die das Ende der Horizontalverkabelung darstellt und die es ermöglicht, PC und Telefon bequem anzuschließen. (In der Praxis umfasst der Begriff »Arbeitsplatz« natürlich das gesamte Büro bzw. die Arbeitsnische.) Die Wandsteckdose besitzt für gewöhnlich zwei Buchsen zum Anschluss der Kabel, eine Befestigungsklammer und eine Abdeckung. Die Verbindung zum PC wird per Patchkabel hergestellt (Abbildung 18.38).



Abb. 18.38: Typische Wandsteckdose eines PC-Arbeitsplatzes

Die weiblichen RJ-45-Buchsen in der Wandsteckdose gehören ebenfalls zu einer bestimmten Kategorie. Sie sollten diese entsprechend der sonstigen Verkabelung des Netzwerks wählen. Tatsächlich verwenden viele Hersteller von Netzwerkanschlüssen in den Wandsteckdosen die gleichen Komponenten wie beim Patchfeld, häufig den 110-Block (Abbildung 18.39). Solche modular aufgebauten Wandsteckdosen erleichtern die Installation deutlich.



Abb. 18.39: Anschließen eines Buchsenmoduls

Jetzt muss nur noch der PC angeschlossen werden, wozu gewöhnlich mehradrige Patchkabel benutzt werden, da diese die Belastungen durch das Umstellen von PCs und die gelegentlichen Fußtritte besser verkraften können.

Beim Arbeitsplatz handelt es sich wohl um den einfachsten Teil der strukturierten Verkabelung, er ist aber gleichzeitig auch die häufigste Fehlerquelle bei Netzwerkstörungen. Falls ein Anwender nicht aufs Netzwerk zugreifen kann und Sie ein defektes Kabel als mögliche Ursache in Betracht ziehen, sollten Sie zunächst den Arbeitsplatz überprüfen.

18.3.3 WAN

In einem *WAN* (*Wide Area Network*, Weitverkehrsnetz) sind die Computer weit verteilt und über Fernleitungen miteinander verbunden. LANs werden durch einen Router zu einem WAN verbunden (Abbildung 18.40). Bestes Beispiel hierfür ist das Internet.



Abb. 18.40: Zwei Broadcast-Domänen werden durch einen Router miteinander verbunden: ein WAN

Sie können mehrere kleine Netzwerke zu einem größeren Netzwerk zusammenschließen, indem Sie aus einer Gruppe von LANs ein WAN machen, allerdings ist dabei hinsichtlich des Datenverkehrs einiges zu beachten. Der Computer benötigt eine leistungsfähige und flexible Methode, um die Frames mit einer Adresse zu versehen, damit diese Frames andere Computer im eigenen LAN oder in einem anderen LAN des WANs erreichen können. Broadcasting ist dafür ungeeignet, jedenfalls zwischen verschieden LANs. Wenn alle Computer jeden Frame untersuchen müssten, würde der Datenverkehr im Netzwerk sehr schnell außer Kontrolle geraten! Die Adressierungsmethode muss außerdem so aufgebaut sein, dass ein Router die Frames sortieren und an das richtige LAN weiterleiten kann. Damit dieser Vorgang, der *Routing* genannt wird, richtig funktioniert, sind Router und Routing-fähige Protokolle erforderlich.

Eingehende Broadcasts werden vom Router verworfen. Dass der Router Broadcastframes nicht weiterleitet, ist Absicht, denn dadurch können innerhalb einer Broadcast-Domäne weiterhin Broadcasts verwendet werden, ohne anderenorts zu stören.

Um Computer jenseits des eigenen LANs zu erreichen, ist ein Netzwerkprotokoll mit Routingfähigkeiten erforderlich – eine Methode, die festlegt, wie die Computer miteinander kommunizieren. Dieses Protokoll, das in der großen Mehrheit aller Netzwerke zum Einsatz kommt, heißt TCP/IP und wird in Kapitel 19 ausführlich beschrieben.

18.4 Wiederholung

18.4.1 Fragen

1. Aus wie vielen Bits besteht eine MAC-Adresse?
   A. 24
   B. 36
   C. 48
   D. 64
2. Welche Kabelkategorie ist für ein 100BaseT-Netzwerk mindestens erforderlich?
   A. CAT1
   B. CAT5
   C. CAT5e
   D. CAT6
3. Welche der genannten Topologien ist eine Hybrid-Topologie?
   A. Bus
   B. Stern
   C. Ring
   D. Stern-Bus
4. Welcher Stecker wird normalerweise für CAT6-Kabel verwendet?
   A. RJ-11
   B. RJ-45
   C. Plenum
   D. PVC
5. Wieso sollte man STP statt UTP verwenden?
   A. STP ist preiswerter.
   B. STP ist einfacher zu installieren.
   C. STP ist weniger empfindlich gegen Interferenzen.
   D. Die beiden Begriffe bezeichnen dasselbe.

6. Welche Frames werden von allen NICs in einem LAN empfangen?
   A. CAT7
   B. Broadcast
   C. WAN
   D. SC, ST oder LC
7. Microsoft Internet Explorer, Mozilla Firefox, Safari, Google Chrome und Microsoft Edge sind was?
   A. Webserver
   B. Druckerserver
   C. Webbrowser
   D. Proxyserver
8. Marks Chef bittet bei der Netzwerkanbindung eines abgelegenen Firmengebäudes, das etwa einen Kilometer vom Hauptgebäude entfernt ist, um Rat. Die dazwischen liegenden Grünflächen gehören dem Unternehmen. Welche Netzwerktechnologie sollte Mark vorschlagen?
   A. Ethernet per UTP
   B. Ethernet per STP
   C. Multimode-Glasfaser-Ethernet
   D. Singlemode-Glasfaser-Ethernet
9. Claudia kommt nicht weiter. Sie möchte Daten vom Laptop ihrer Freundin auf ihrem Desktop bearbeiten, hat jedoch keinen USB-Speicherstick zur Hand. Ihr stehen zwar verschiedene Ethernet-Kabel zur Verfügung, aber alle Ports des Switches sind belegt. Was könnte sie in dieser Situation tun?
   A. Die Computer mit einem Patchkabel direkt verbinden.
   B. Die beiden Computer mit einem Crossover-Kabel direkt verbinden.
   C. Die beiden Computer mit einem STP-Kabel direkt verbinden.
   D. Im Computerladen um die Ecke einen USB-Speicherstick kaufen und die Daten damit übertragen.
10. Herbert gibt Stefan ein Kabel. Stefan gibt es ihm zurück und sagt wissend: »Schicker Typ-F-Stecker!« Welche Art Kabel hat Herbert?
   A. Koaxialkabel
   B. Glasfaserkabel
   C. STP-Kabel
   D. UTP-Kabel

18.4.2 Antworten

1. **C.** MAC-Adressen sind 48 Bit lang.
2. **B.** Die 100Base-T-Netzwerke benötigen mindestens CAT5-Kabel.
3. **D.** Die Stern-Bus-Topologie, die bei Ethernet-Netzwerken zum Einsatz kommt, ist eine Hybrid-Topologie.
4. **B.** Bei CAT6-Kabeln werden RJ-45-Stecker verwendet.
5. **C.** STP-Kabel sind weniger empfindlich gegen Interferenzen als UTP-Kabel.
6. **B.** Alle NICs in einem LAN empfangen Broadcastframes.
7. **C.** Bei all diesen Programmen handelt es sich um Webbrowser.

8. **D.** Mark sollte die einzige der hier genannten Methoden vorschlagen, die solche Distanzen überbrücken kann, nämlich Singlemode-Glasfaser-Ethernet.
9. **B.** Claudia sollte die beiden Computer mit einem Crossover-Kabel direkt miteinander verbinden.
10. **A.** Herbert hat ein richtig schickes Koaxialkabel.

Lokale Netzwerke | 19

Themen in diesem Kapitel:

- TCP/IP-Grundlagen
- Kabelgebundene Netzwerke installieren und konfigurieren
- Fehlersuche in kabelgebundenen Netzwerken

Netzwerke dominieren das moderne Computerumfeld. Unmengen der im Geschäftsbereich genutzten Rechner sind in kleinen lokalen Netzwerken (*LAN – Local Area Network*) miteinander verbunden und Großunternehmen können heute nicht mehr überleben, ohne ihre vielen Büros zu einem großen WAN (*Wide Area Network*) zu verbinden.

Hinweis

In diesem Kapitel werden ausschließlich lokale Netzwerke vorgestellt, wie etwa eine Gruppe von Computern in einem einzelnen Büro. Die Verbindungsaufnahme mit dem Internet hebe ich mir für Kapitel 21 auf, also halten Sie sich bereit! Sie sollten sich alle Inhalte dieses Kapitels zu eigen machen, bevor Sie den nächsten Schritt wagen und sich mit dem Internet verbinden.

Netzwerke sind heute derart verbreitet, dass jeder gute Techniker die Grundlagen der Netzwerktechnologien, der Betriebssysteme, der verschiedenen Implementationen und der Problembehebung kennen muss. Entsprechend werden Sie in diesem Kapitel lernen, wie Sie ein einfaches Netzwerk einrichten und dabei auftretende Probleme beheben können.

Zunächst sehen wir uns TCP/IP näher an und wie Windows es in einem typischen Netzwerk verwendet. Alle modernen Netzwerke verwenden zur Kommunikation das TCP/IP-Protokoll, deshalb müssen Sie wissen, wie es funktioniert.

Anschließend werden wir von Grund auf ein kleines Netzwerk einrichten. Dazu gehört dessen Planung, die Installation und Konfiguration von Netzwerkkarten, Switches und TCP/IP. Kurz: Alles, was benötigt wird, um Ordner, Drucker, Bibliotheken usw. freizugeben.

Dieses Kapitel endet mit der Fehlersuche im Netzwerk. Moderne Betriebssysteme verfügen für den Fall, dass das Netzwerk nicht funktioniert, über eine Reihe hilfreicher Werkzeuge. Diese werden wir uns ansehen und mit einem Plan zur Fehlersuche kombinieren, um das Netzwerk wieder zum Laufen zu bringen.

1001/1002

19.1 TCP/IP

Wie Sie aus Kapitel 18, *Netzwerk: Grundlagen*, wissen, erledigt das Ethernet-Protokoll die Aufgabe, Daten von einem Rechner zum anderen zu transportieren. Aber Ethernet allein reicht zum Aufbau eines kompletten Netzwerks nicht aus. Beispielsweise kann ein Ethernet-Frame maximal 1.500 Byte enthalten. Wenn aber die zu transportierenden Daten größer als 1.500 Byte sind, was dann? Irgendwie müssen die Daten an einem Ende einer Verbindung in kleinere Häppchen aufgeteilt und am anderen Ende wieder zusammengesetzt werden, damit sie genutzt werden können.

Eine weitere Schwierigkeit ergibt sich, wenn bei einem der mit dem Netzwerk verbundenen Computer die Netzwerkkarte ersetzt wird. Bislang stellt die MAC-Adresse der Netzwerkkarte die einzige

Möglichkeit dar, die einzelnen Rechner voneinander zu unterscheiden. Um dieses Problem zu beheben, muss jedem Rechner im Netzwerk ein eindeutiger Name zugewiesen werden, der nicht auf der MAC-Adresse beruht. Und irgendwie muss nachverfolgt werden, welche MAC-Adresse zu welchem Rechnernamen gehört, damit die Ethernet-Frames richtig zugeordnet werden können. Wenn man die Netzwerkkarte eines Computers austauscht, wird das Netzwerk die neue MAC-Adresse in die Liste der PC-Namen und der zugehörigen MAC-Adressen aufnehmen (nach entsprechenden Anfragen).

Die Netzwerkprotokoll-Software organisiert die von den Netzwerkkarten gelieferten Daten, übergibt sie an die Anwendung, die sie benötigt, und leitet die von der Anwendung bereitgestellten Daten an die Netzwerkkarte weiter, die sie über das Netzwerk versendet. Alle Netzwerke verwenden irgendein Netzwerkprotokoll. Im Laufe der Jahre gab es eine Vielzahl von Protokollen, die zumeist mehrere einfache Protokolle zu einem sogenannten *Protokollstack* zusammenfassten. Diese Vorgehensweise führte dazu, dass einige Protokolle einen ziemlich verrückten Namen besitzen, wie z.B. TCP/IP.

Das *Transmission Control Protocol/Internet Protocol* (*TCP/IP*) ist das vorwiegend in modernen Netzwerken eingesetzte Protokoll. Damit ein PC auf das Internet zugreifen kann, muss TCP/IP geladen und korrekt konfiguriert sein. Sehen wir uns also einige Aspekte des TCP/IP-Protokollstacks an!

19.1.1 Netzwerk-Adressierung mit IPv4

Alle Netzwerkadressen müssen zwei Arten von Informationen enthalten. Sie müssen einen Rechner eindeutig identifizieren und ihn in einem größeren Netzwerk ausfindig machen können. In einem TCP/IP-Netzwerk identifiziert die *IP-Adresse* den Rechner innerhalb eines Netzwerks. Sie können der IP-Adresse jedoch nicht ansehen, welcher Teil davon das Netzwerk und welcher den einzelnen Computer festlegt.

IP-Adressen

Bei der IP-Adresse handelt es sich um die eindeutige numerische Kennung eines Systems in einem Netzwerk. Die meisten Systeme verwenden derzeit noch das Adressschema gemäß *Internet Protocol version 4* (*IPv4*). IPv4-Adressen bestehen aus vier Gruppen mit je acht Binärziffern (Oktette), die jeweils durch einen Punkt getrennt werden (*dotted-decimal notation*). Statt einem Rechner also einen Namen, wie z.B. `SERVER1` zu geben, erhält er eine Adresse wie diese:

```
202.34.16.11
```

Schreibt man diese binär, erhält man die Adresse

```
11001010.00100010.00010000.00001011
```

Statt die Adressen binär zu schreiben, haben sich die TCP/IP-Entwickler der besseren Lesbarkeit halber dazu entschlossen, die dezimalen Äquivalente zu verwenden:

```
00000000 = 0
00000001 = 1
00000010 = 2
...
11111111 = 255
```

Subnetzmaske

Ein Teil der IP-Adresse legt das Netzwerk fest (die Netzwerk-ID) und ein weiterer Teil identifiziert den lokalen Compter (die Host-ID bzw. der Host). Die Netzwerkkarten verwenden die sogenannte *Subnetzmaske* um zu bestimmen, welcher Teil der IP-Adresse als Netzwerkadresse und welcher als Host-Adresse dient. Die Subnetzmaske blockiert (oder »maskiert«) den Netzwerkteil einer IP-Adresse.

Betrachten wir eine typische Subnetzmaske: 255.255.255.0. Der Teil 255.255.255 maskiert die Netzwerk-ID, die 0 am Ende die Host-ID. Ein Beispiel: IP-Adresse 192.168.4.33 und Subnetzmaske 255.255.255.0. Die ersten drei Oktette der Subnetzmaske lauten 255, daher ist die Netzwerk-ID 192.168.4 und die eindeutige Host-ID 33.

In einem einzelnen LAN besitzen alle Computer dieselbe Netzwerk-ID und eine eindeutige Host-ID. Das heißt, dass in diesem Netzwerk alle IP-Adressen mit 192.168.4 beginnen. Andererseits muss jeder Computer eine eindeutige Host-ID besitzen. Falls zwei Computer dieselbe IP-Adresse verwenden, können diese nicht miteinander kommunizieren und andere Computer wären nicht in der Lage, ihnen Daten zu senden. Man bezeichnet das als *Adresskonflikt*.

Eine IP-Adresse darf nicht mit einer 0 oder mit 255 enden, im Beispiel gibt es somit IP-Adressen im Bereich von 192.168.4.1 bis 192.168.4.254, also insgesamt 254 IP-Adressen.

Ursprünglich wurden Subnetze entsprechend der Anzahl der Oktette in der Subnetzmaske in Klassen wie A, B und C unterteilt. Eine Adresse der Klasse C, wie die eben erwähnte, besitzt die Subnetzmaske 255.255.255.0, eine Adresse der Klasse B hingegen 255.255.0.0. Bei einer Adresse der Klasse B stehen also zwei Oktette (16 Bits) für Hosts zur Verfügung. In einem Netzwerk der Klasse B gibt es somit 2^{16}-2 = 65.534 eindeutige Host-IDs.

Subnetzmasken werden zwar noch immer oft als Gruppe von dreimal »255« angegeben, das Klassensystem ist aber längst Geschichte. Da es sich bei der Subnetzmaske um eine Binärzahl handelt, kann man Subnetze mit einer beliebigen Anzahl von Einsen in der Subnetzmaske erstellen.

Das gegenwärtig verwendete System trägt den Namen *CIDR* (*Classless Inter-Domain Routing*). Hier können auch leicht Binärzahlen benutzt werden, wenngleich es auch ein wenig unschön aussieht, wenn man die Zahlen als Oktette aufschreibt. Ein einfaches Beispiel soll das illustrieren. Die Subnetzmaske 255.255.255.0 sieht in der Binärnotation so aus:

```
11111111.11111111.11111111.00000000
```

In der CIDR-Nomenklatur kann die Anzahl der Einsen in der Subnetzmaske direkt angegeben werden. Die gerade genannte Subnetzmaske enthält beispielsweise 24 Einsen und würde als `/24` notiert, wodurch 254 Host-IDs verfügbar wären. Man spricht dann von einem `/24`-Netzwerk.

Wenn Sie eine Netzwerk-ID verwenden möchten, die mehr Host-IDs ermöglicht, müssen Sie eine Subnetzmaske mit weniger Einsen verwenden, so wie diese hier:

```
11111111.11111111.11110000.00000000
```

Zählen Sie die Einsen – es sind 20. Die Einsen maskieren die Netzwerk-ID. Damit verbleiben 12 Stellen für die Host-ID und somit sind $2^{12} - 2 = 4094$ eindeutige Host-IDs in einem `/20`-Netzwerk verfügbar.

Wenn Sie die Binärzahlen (die Einser-Ketten) in Oktette umrechnen, erhalten Sie Folgendes:

```
255.255.240.0
```

Es mag ungewohnt aussehen, aber hierbei handelt es sich um eine vollkommen korrekte Subnetzmaske, auch wenn die Darstellung als Binärzahl offensichtlicher ist.

Aus praktischer Sicht müssen Sie als Techniker lediglich wissen, wie Sie einen Computer so konfigurieren, dass er die IP-Adresse und die Subnetzmaske übernimmt, die Ihr Netzwerkadministrator Ihnen mitteilt.

Wichtig

Den grundlegenden Unterschied zwischen Subnetzmaske und CIDR-Nomenklatur sollten Sie kennen.

Netzwerke per Router verbinden

Abbildung 19.1 zeigt ein typisches LAN, wie man es in Haushalten oder kleinen Büros findet. Jedes Gerät in diesem Netzwerk besitzt eine IP-Adresse, die in diesem Fall 192.168.4.x lautet, wobei x ein eindeutiger Wert zwischen 1 und 254 sein muss (0 und 255 sind reserviert). Alle IP-Adressen fangen also mit 192.168.4 an, und das ist die Netzwerk-ID dieses LANs. Beachten Sie, dass jedes Gerät eine eindeutige IP-Adresse besitzt, die jedoch stets mit 192.168.4 beginnt. Die Subnetzmaske 255.255.255.0 teilt dem System mit, dass die ersten drei Zahlen übereinstimmen müssen (jeweils die 255) und die letzte Zahl (die 0) einen beliebigen gültigen Wert annehmen darf.

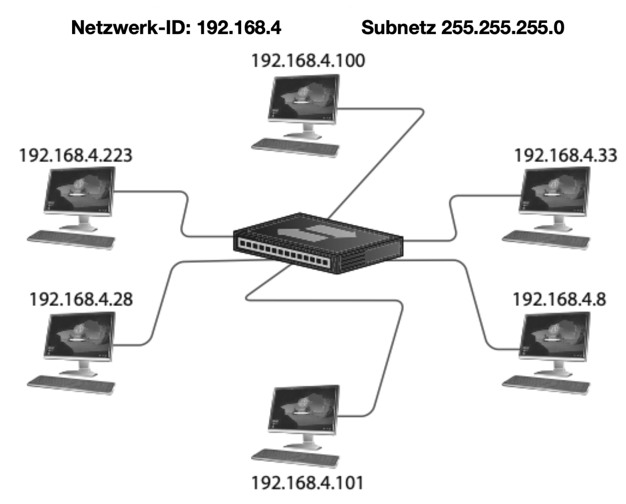


Abb. 19.1: Ein LAN mit Netzwerk-ID und Subnetzmaske

Die IP-Adressierung ermöglicht es, mehrere Netzwerke anhand der Netzwerk-ID miteinander zu verbinden und so ein größeres Netzwerk zu bilden, das WAN (*Wide Area Network*) genannt wird. In einem LAN sind die Systeme über einen Switch miteinander verbunden, der anhand der MAC-Adressen filtert und weiterleitet. Für die Verbindung mehrerer Netzwerke ist ein Gerät erforderlich, nämlich ein Router, der anhand von IP-Adressen filtert und weiterleitet. Der Netzwerkanschluss Ihres Routers, der mit Ihrem LAN verbunden ist, erhält eine IP-Adresse mit einer Netzwerkadresse, die derjenigen Ihres LANs entspricht. Diese Adresse verwendet Ihr Computer, um Daten an Adressen zu versenden, die sich außerhalb Ihres LANs befinden. Abbildung 19.2 zeigt einen typischen Router, der in kleinen Büros zum Einsatz kommt.



Abb. 19.2: Typischer SOHO-Router

Ein Router besitzt mindestens zwei Netzwerkanschlüsse, damit er mit zwei verschiedenen LANs verbunden werden kann. Jedes mit dem Internet verbundene LAN verwendet einen Router wie den in Abbildung 19.2. Einer der Anschlüsse des Routers ist mit dem Switch Ihres lokalen Netzwerks und der andere mit einem weiteren Netzwerk verbunden, für gewöhnlich mit dem Ihres Internetanbieters, das wiederum mit Millionen anderer Router und Milliarden anderer Computer verbunden ist (Abbildung 19.3). Die IP-Adresse des Netzwerkanschlusses Ihres Routers, die mit dem lokalen Netzwerk verbunden ist, wird *Standardgateway* (oder manchmal auch *Standardrouter*) genannt.

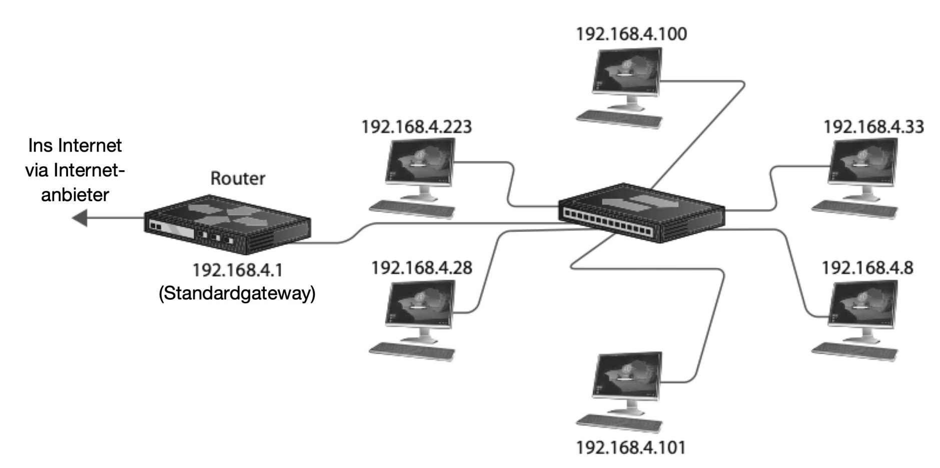


Abb. 19.3: Standardgateway

Domain Name System (DNS) Wohl wissend, dass sich die Anwender IP-Adressen nicht merken können, haben die Internet-Pioniere eine Möglichkeit entwickelt, diesen Zahlenkombinationen anwenderfreundlichere Rechnerbezeichnungen zuzuordnen. Spezielle Rechner, die sogenannten *DNS-Server*, enthalten Datenbanken mit den IP-Adressen und den zugewiesenen Namen. Ein Rechner mit dem Namen `www.totalsem.com` wird z.B. in einem DNS-Verzeichnis mit der zugehörigen IP-Adresse (z.B. 209.34.45.163) geführt. Statt beim Aufruf einer Webseite `http://209.34.45.163` eingeben zu müssen, können Sie so die Adresse `www.totalsem.com` verwenden. Ihr System erfragt dann die IP-Adresse von `www.totalsem.com` beim DNS-Server und verwendet diese dann, um den richtigen Rechner ausfindig zu machen. Wenn Sie nicht immer IP-Adressen eintippen wollen, dann benötigen alle TCP/IP-Netzwerke mindestens einen DNS-Server (Abbildung 19.4).

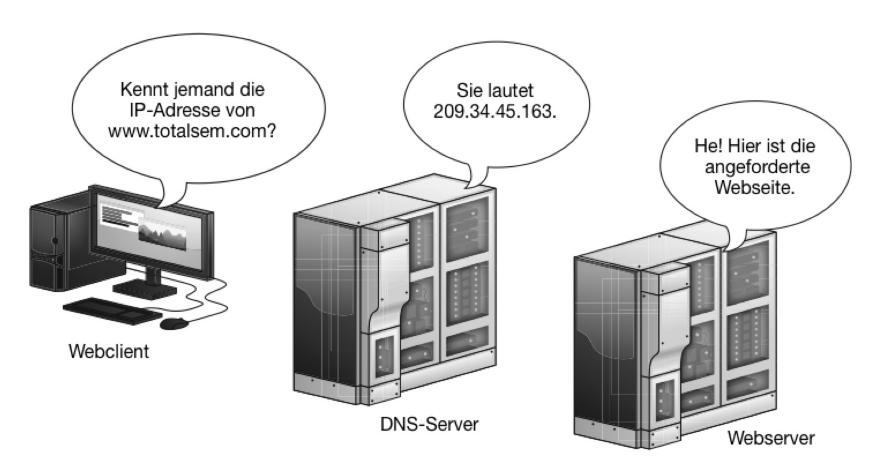


Abb. 19.4: Das Domain Name System

Hinweis

Heutzutage beherbergen die meisten Webserver mehrere Websites unter derselben IP-Adresse. Es wird immer schwieriger, auf eine bestimmte Website per IP-Adresse zuzugreifen. Beispielsweise verweist die in den Beispielen genannte IP-Adresse nicht auf unsere Website. Fort mit euch, Hacker!

Die Domänennamen im Internet folgen sehr strengen Regeln. Wenn Sie einen Domänennamen haben wollen, über den Sie für andere Teilnehmer im Internet erreichbar sind, müssen Sie diesen registrieren lassen und dafür eine geringe jährliche Gebühr entrichten. Ursprünglich hatten alle DNS-Namen eine der folgenden sieben Endungen, die *Top Level Domains* (TLD) genannt werden:

.com	Allgemeine Geschäftsadresse (»commercial«)
.edu	Bildungseinrichtungen (»education«)
.gov	Regierungsbehörden (»government«)
.int	Internationale Adressen
.mil	Militärorganisationen
.net	Internetorganisationen
.org	Gemeinnützige Organisationen

Mit den zunehmend am Internet teilnehmenden Ländern wurde eine komplett neue Domänenebene hinzugefügt, die für das jeweilige Land steht (z.B. `.de` für Deutschland oder `.ch` für die Schweiz). Die ursprünglichen sieben Endungen werden aber weiterhin unterstützt. Häufig begegnet man DNS-Namen wie z.B. `www.bbc.co.uk` (BBC Großbritannien) oder `www.louvre.fr` (der Louvre in Frankreich). Die ICANN (*Internet Corporation for Assigned Names and Numbers*) hat eine Reihe weiterer Domänen hinzugefügt (u.a. `.name`, `.biz`, `.info`, `.tv` und andere).

TCP/IP konfigurieren Wenn Sie die Netzwerkverbindung Ihres Computers manuell konfigurieren, müssen Sie IP-Adresse, Subnetzmaske, Standardgateway und mindestens einen DNS-Server eintragen. Noch mal im Einzelnen:

- **IP-Adresse**: Die eindeutige Netzwerkadresse des Computers
- **Subnetzmaske**: Legt Ihre Netzwerkadresse fest
- **Standardgateway**: Die IP-Adresse Ihres lokalen Routers
- **DNS-Server**: Ermöglicht die Verwendung leicht zu merkender DNS-Namen für IP-Adressen

Die Konfiguration der TCP/IP-Einstellungen ist auf zweierlei Weise möglich: statisch oder dynamisch. Abbildung 19.5 zeigt die Konfiguration auf einem System mit Windows 10. Hier können Sie statische Informationen eingeben.

Beim Betrachten von Abbildung 19.5 ist Ihnen vielleicht aufgefallen, dass es dort den Punkt IP-Adresse automatisch beziehen gibt. Hierbei handelt es sich um eine häufige Einstellung, bei der Sie keine weiteren Daten eintragen müssen. Sie können diese Einstellung verwenden, um automatisch eine IP-Adresse von einem DHCP-Server (*Dynamic Host Configuration Protocol*) im Netzwerk zu beziehen. Wenn in Ihrem Netzwerk ein DHCP-Server vorhanden ist (in den meisten Netzwerken ist das der Fall) und Sie Ihren Computer entsprechend konfiguriert haben, sendet er beim Start eine DHCP-Anfrage. Der DHCP-Server liefert Ihrem Rechner dann alle erforderlichen Informationen, um ins Netzwerk zu gelangen (Abbildung 19.6).

Sie können übrigens auch selbst eine Adresse eingeben, um so eine *statische IP-Adresse* zu erzeugen. Statisch bedeutet, dass die Adresse unverändert bleibt, sofern Sie selbst oder ein anderer Techniker sie nicht ändern.

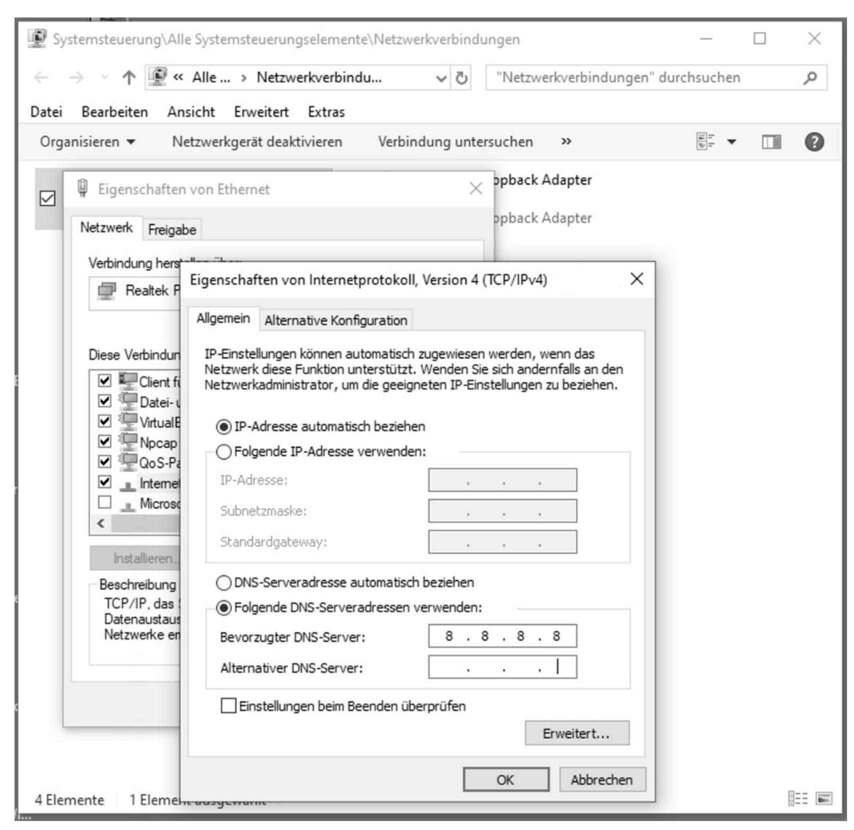


Abb. 19.5: Die IP-Einstellungen unter Windows 10

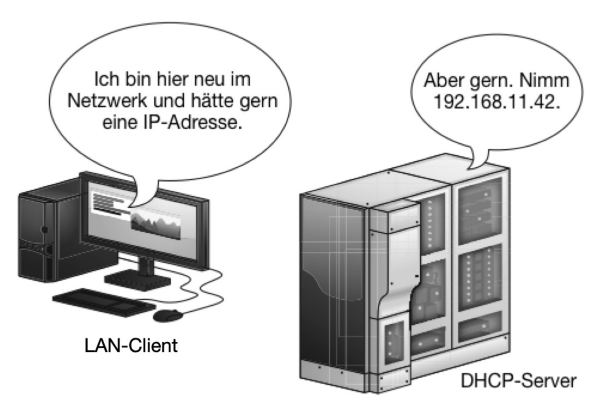


Abb. 19.6: Der DHCP-Server vergibt eine IP-Adresse.

Wichtig

Netzwerkadministratoren richten DHCP-Server so ein, dass bestimmte Adressen für spezielle Aufgaben reserviert sind, beispielsweise für andere Server oder Drucker. Normalerweise sind die IP-Adressen aller Server reserviert. In einem kleinen Netzwerk werden üblicherweise `.1` für das Standardgateway und `.2` bis `.9` für andere Server reserviert.

TCP/UDP

Bei der Datenübertragung zwischen zwei Systemen muss TCP/IP wissen, ob es sich um eine verbindungsorientierte oder verbindungslose Kommunikation handelt. Wenn man sichergehen möchte, dass die transportierten Daten in ordnungsgemäßer Reihenfolge beim anderen System ankommen, verwendet man verbindungsorientierte Kommunikation. Wenn es hingegen nicht darauf ankommt, ob hier und da mal ein Bit verloren geht, ist verbindungslose Kommunikation die erste Wahl. Das bei TCP/IP verwendete verbindungsorientierte Protokoll heißt *TCP* (*Transmission Control Protocol*). Das verbindungslose wird als *UDP* (*User Datagram Protocol*) bezeichnet.

Ich möchte das klarstellen: Es ist nicht so, dass Sie auswählen können, ob TCP oder UDP verwendet wird. Das haben die Entwickler der zum Einsatz kommenden Programme bereits entschieden. Wenn Sie beispielsweise einen Webbrowser starten, verwendet dieser TCP, weil er das Protokoll HTTP benutzt, und das beruht auf TCP.

Wichtig

Rechnen Sie in der Zertifizierungsprüfung mit Fragen, die sich auf den Unterschied von TCP und UDP beziehen. Merken Sie sich *verbindungsorientiert* und *verbindungslos*, dann werden Sie die richtige Antwort geben können.

Mehr als 95% aller TCP/IP-Anwendungen verwenden TCP. TCP sorgt für eine verlässliche und vollständige Datenübertragung von einer Maschine zur anderen. Daher gibt es bei TCP Kommunikationsvorschriften, die verlangen, dass sowohl die sendende als auch die empfangende Maschine die Bereitschaft seines Gegenübers, Daten zu senden und zu empfangen, bestätigt.

UDP geht eher nach dem Muster »abschicken und nicht mehr daran denken« vor. Die bei TCP erforderlichen Erweiterungen zum Bestätigen des Empfangs intakter Daten gibt es bei UDP nicht. Am geeignetsten ist UDP für große Datenmengen, bei denen einige Übertragungsfehler nicht entscheidend sind, oder bei Geräten, die so nah beieinanderstehen, dass Übertragungsfehler so unwahrscheinlich sind, dass man sich darüber keine Gedanken macht. Einige fehlende Frames bei einem Gespräch per Voice over IP beispielsweise werden auf die Kommunikation der Gesprächspartner wohl kaum einen Einfluss haben. In diesem Fall gibt es einen guten Grund, UDP zu verwenden: Im Vergleich zu TCP ist UDP rasend schnell.

Hinweis

Es gibt noch einige weitere prüfungsrelevante TCP/IP-Protokolle, die andere Ziele verfolgen. Sie werden allesamt in Kapitel 21 erläutert.

TCP/IP-Dienste

TCP/IP unterscheidet sich von anderen Protokollen. Es unterstützt Datei- und Druckerfreigaben, bietet aber auch eine Reihe zusätzlicher einzigartiger Merkmale. Diese werden unter dem Oberbegriff *TCP/IP-Dienste* zusammengefasst. Der bekannteste TCP/IP-Dienst, bei dem es sich um die Sprache des World Wide Web handelt, wird *HTTP* (*Hypertext Transfer Protocol*) genannt. Wenn Sie im Internet surfen wollen, muss TCP/IP installiert sein. TCP/IP stellt aber neben HTTP viele weitere Dienste zur Verfügung. Mit einem Dienst, der SSH (*Secure Shell*) genannt wird, können Sie auf das Terminal entfernter Rechnersysteme zugreifen, als ob Sie direkt davor säßen.

Das Ziel von TCP/IP ist die Verbindung von zwei Hosts, entweder im selben LAN oder über ein anderes Netzwerk innerhalb des WANs. Die LANs innerhalb des WANs werden über die unterschiedlichsten Verbindungen verknüpft, von einfachen Einwahlnetzen bis hin zu dedizierten, schnellen (und teuren) Datenleitungen (Abbildung 19.7). Zur Übertragung des Datenverkehrs zwischen Netzwerken werden *Router* eingesetzt (Abbildung 19.8). Jeder Host sendet Daten nur dann zum Router, wenn sie

für ein entferntes Netzwerk vorgesehen sind, was den Datenverkehr über die teureren WAN-Verbindungen reduziert. Der Host entscheidet darüber anhand der Ziel-IP-Adressen der einzelnen Pakete.

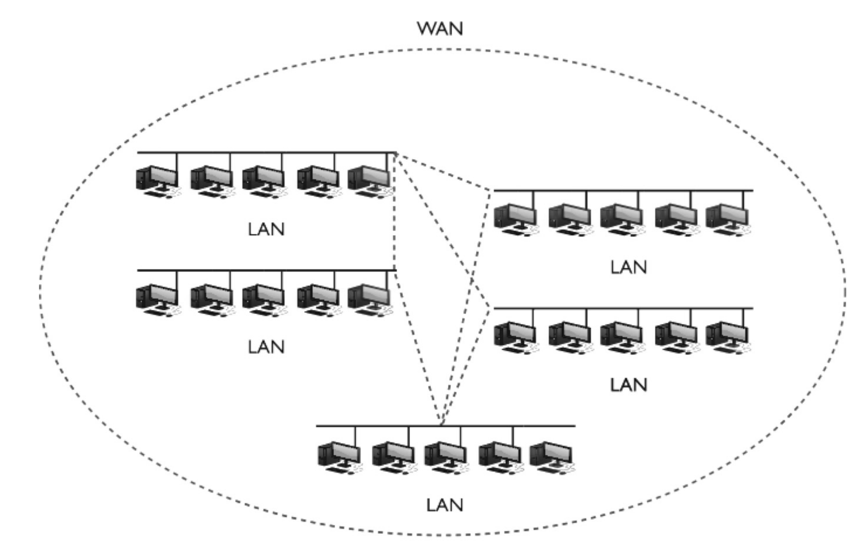


Abb. 19.7: Das WAN-Konzept

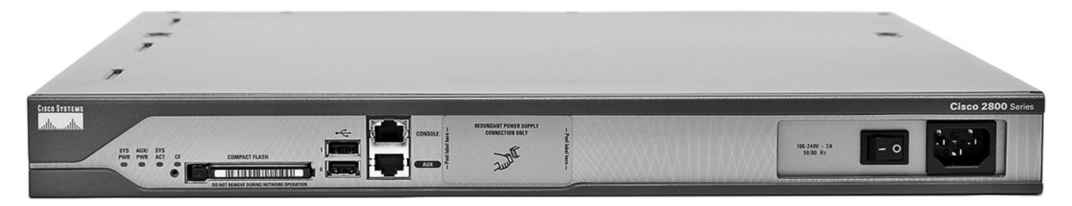


Abb. 19.8: Ein typischer Router

TCP/IP-Einstellungen

Für TCP/IP sind eine Reihe spezieller Einstellungen erforderlich, die korrekt vorgenommen werden müssen, wenn das Netzwerk ordnungsgemäß funktionieren soll. Leider sind diese Einstellungen ein wenig verwirrend und es gibt doch etliche davon. Nicht alle Einstellungen werden für die verschiedenen Arten von TCP/IP-Netzwerken benötigt und es ist auch nicht immer ganz offensichtlich, wo sie vorgenommen werden müssen.

Unter Windows wird die Konfiguration mit dem Applet NETZWERKVERBINDUNGEN vorgenommen. Sie gelangen dorthin, wenn Sie im Startmenü NETZWERVERBINDUNGEN anklicken oder in der Systemsteuerung das NETZWERK- UND FREIGABECENTER auswählen. Anschließend markieren Sie dann die zu konfigurierende Verbindung und wählen nach einem Rechtsklick im Kontextmenü die Option EIGENSCHAFTEN, um zu den Eigenschaften für das Internetprotokoll (TCP/IP) zu gelangen. In Windows 10 können Sie auch EINSTELLUNGEN|NETZWERK UND INTERNET|STATUS öffnen und dort ADAPTEROPTIONEN ÄNDERN anklicken, um die vorhandenen Netzwerkkarten anzuzeigen.

Die CompTIA A+-Zertifizierung geht davon aus, dass Ihnen die richtigen und erforderlichen Einstellungen für das Netzwerk von einem Techniker oder einem Netzwerkfachmann mitgeteilt werden. Sie müssen daher nur ungefähr wissen, was die verschiedenen Einstellungen bewirken und wo Sie diese vornehmen müssen, wenn das System funktionieren soll.

TCP/IP-Hilfsprogramme

Alle modernen Betriebssysteme enthalten praktische Hilfsprogramme zum Testen und Konfigurieren von TCP/IP. Die Hilfsprogramme, die in diesem Bereich besonders häufig eingesetzt werden, sind `ping`, `ipconfig`, `ifconfig`, `nslookup`, `tracert` und `traceroute`. Alle diese Programme werden von der Kommandozeile aus gestartet. Öffnen Sie eine Eingabeaufforderung, um sie auszuführen.

ping Mit ping lässt sich feststellen, ob zwei Systeme miteinander kommunizieren können. Sie können es folgendermaßen nutzen. Öffnen Sie die Eingabeaufforderung oder ein Terminal und geben Sie `ping` gefolgt von einem Leerzeichen und einer IP-Adresse oder einem DNS-Namen ein, also z.B. `ping www.totalsem.com`. Betätigen Sie ↵ und das war's auch schon! Abbildung 19.9 zeigt die allgemeine Syntax von `ping`.

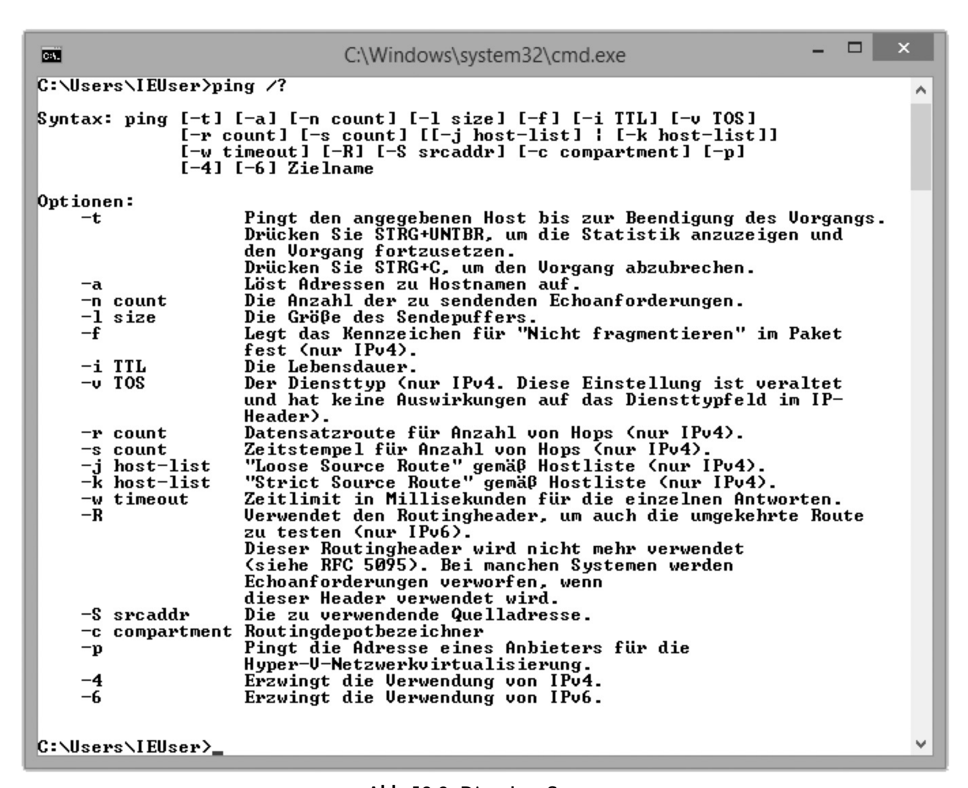


Abb. 19.9: Die `ping`-Syntax

Der `ping`-Befehl kennt ein paar Optionen, die über die Grundlagen hinausgehen. Die erste ist `-t`. Wenn dieser Schalter verwendet wird, dann sendet der Befehl fortwährend `ping`-Pakete, bis Sie das Programm mit der Tastenkombination Strg + C abbrechen. In macOS und Linux ist das die Voreinstellung; drücken Sie Strg + C, um abzubrechen. Bei der zweiten Option handelt es sich um den Schalter `-l`, mit dem Sie die Größe der zu übertragenden Pakete festlegen können. Das kann bei der Diagnose bestimmter Probleme mit den Routern zwischen Ihrem und dem angepingten Rechner hilfreich sein.

ipconfig/ifconfig Windows bietet das Befehlszeilenwerkzeug `ipconfig` an, mit dem Sie sich einen schnellen Überblick über Ihre Netzwerkeinstellungen verschaffen. Geben Sie auf der Kommandozeile `ipconfig /all` ein, um sich alle Ihre TCP/IP-Einstellungen anzeigen zu lassen (Abbildung 19.10). In macOS und Linux leistet der Befehl `ifconfig` dasselbe, wenn Sie ihn ohne Parameter aufrufen.

```
Eingabeaufforderung

C:\Users>ipconfig /all

Windows-IP-Konfiguration

   Hostname  . . . . . . . . . . . . : KLPC
   Primäres DNS-Suffix . . . . . . . :
   Knotentyp . . . . . . . . . . . . : Hybrid
   IP-Routing aktiviert  . . . . . . : Nein
   WINS-Proxy aktiviert  . . . . . . : Nein
   DNS-Suffixsuchliste . . . . . . . : fritz.box

Ethernet-Adapter Ethernet:

   Medienstatus. . . . . . . . . . . : Medium getrennt
   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physische Adresse . . . . . . . . : 7C-D3-0A-00-19-AC
   DHCP aktiviert. . . . . . . . . . : Ja
   Autokonfiguration aktiviert . . . : Ja

Ethernet-Adapter VirtualBox Host-Only Network:

   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physische Adresse . . . . . . . . : 0A-00-27-00-00-13
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   Verbindungslokale IPv6-Adresse  . : fe80::119d:146b:1876:4c57%19(Bevorzugt)
   IPv4-Adresse  . . . . . . . . . . : 192.168.56.1(Bevorzugt)
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . :
   DHCPv6-IAID . . . . . . . . . . . : 520749095
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-1E-4F-D3-13-7C-D3-0A-00-19-AC

   DNS-Server  . . . . . . . . . . . : fec0:0:0:ffff::1%1
```

Abb. 19.10: Ausgabe von `ipconfig /all` in Windows 10

Wenn Ihr Rechner eine statische IP-Adresse besitzt, zeigt `ipconfig` nicht sehr viel mehr als die aktuellen IP-Einstellungen an, wie beispielsweise IP-Adresse, Subnetzmaske, Standardgateways, DNS-Server und WINS-Server. Wenn Sie dagegen DHCP verwenden, ist `ipconfig` auch das wichtigste Werkzeug, um Ihre IP-Adresse freizugeben und zu erneuern. Sie geben einfach `ipconfig /renew` ein, um eine neue IP-Adresse zu erhalten, oder `ipconfig /release`, um die aktuelle IP-Adresse freizugeben.

nslookup `nslookup` ist ein mächtiges Befehlszeilenprogramm, das es Ihnen ermöglicht, herauszufinden, welche Informationen ein DNS-Server über einen bestimmten Host besitzt. Wenn TCP/IP installiert ist, steht `nslookup` in allen modernen Betriebssystemen zur Verfügung. Um das Programm zu starten, geben Sie `nslookup` auf der Kommandozeile ein und betätigen ↵ (Abbildung 19.11). Beachten Sie, dass anschließend kaum Informationen angezeigt werden. Haben Sie aber bemerkt, dass sich die Eingabeaufforderung geändert hat? Das liegt daran, dass Sie jetzt ein Programm ausführen. Um wieder zur normalen Eingabeaufforderung zurückzukehren, geben Sie `exit` ein und betätigen ↵.

Hinweis

Mit `nslookup` lassen sich ein paar wirklich interessante Dinge anstellen, daher lieben manche Techniker dieses Werkzeug. Geben Sie `help` auf der `nslookup`-Eingabeaufforderung ein und drücken Sie ↵, um sich eine Liste der Befehle und deren Syntax anzeigen zu lassen.

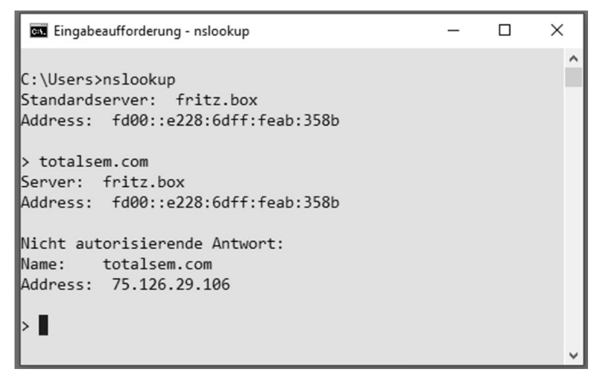


Abb. 19.11: Der Befehl `nslookup` in Aktion

tracert/traceroute Die Werkzeuge `tracert` (Windows) und `traceroute` (macOS und Linux) zeigen die Route an, die ein Paket auf dem Weg zu seinem Ziel nimmt. Geben Sie auf der Kommandozeile einfach `tracert` bzw. `traceroute` und anschließend ein Leerzeichen sowie eine IP-Adresse ein. Die Ausgabe beschreibt die Route vom lokalen Rechner zum Zielrechner und führt alle Geräte auf, die ein Datenpaket durchläuft, und wie lange die einzelnen Sprünge dabei dauern (Abbildung 19.12). `tracert` kann nützlich sein, wenn es darum geht, Engpässe zu beheben. Wenn sich die Anwender darüber beklagen, dass bestimmte Zieladressen bei Verwendung von TCP/IP schwer zu erreichen sind, dann können Sie das Hilfsprogramm starten und damit feststellen, ob das Problem bei einem Rechner besteht, der unter Ihrer Aufsicht steht, oder ob es sich um ein Problem bei einem anderen Rechner oder Router handelt. Wenn eine Zieladresse überhaupt nicht erreichbar ist, können Sie `tracert` ebenfalls einsetzen, um festzustellen, ob das Problem von einem Rechner oder Router verursacht wird, der unter Ihrer Aufsicht steht.

```
Eingabeaufforderung

C:\Users>tracert google.com

Routenverfolgung zu google.com [2a00:1450:4001:81b::200e]
über maximal 30 Hops:

  1     1 ms     1 ms     1 ms  fritz.box [2003:e3:c718:200:e228:6dff:feab:358b]
  2    18 ms    18 ms    18 ms  2003:0:8403:f000::1
  3     *        *        *     Zeitüberschreitung der Anforderung.
  4    25 ms    24 ms    24 ms  2003:0:1304:800f::2
  5    25 ms    25 ms    25 ms  2a00:1450:80f8::1
  6    27 ms    25 ms    25 ms  2001:4860:0:1::692
  7    25 ms    24 ms    24 ms  2001:4860:0:1::673
  8    24 ms    25 ms    24 ms  fra15s16-in-x0e.1e100.net [2a00:1450:4001:81b::200e]

Ablaufverfolgung beendet.

C:\Users>
```

Abb. 19.12: Der Befehl `tracert` in Aktion

Tipp: Ausführung von `tracert/traceroute`

Haben Sie sich auch schon gefragt, warum der E-Mail-Versand an manche Empfänger ewig dauert, an andere hingegen blitzschnell vonstattengeht? Oder warum das Laden einer Webseite so viel länger dauert als das einer anderen? Zum Teil kann es daran liegen, wie viele Sprünge zwischen Ihnen und dem Zielser-

ver liegen. Mit `tracert/traceroute` können Sie feststellen, wie viele Stationen die Datenpakete durchlaufen müssen, bis sie ihr Ziel im Netzwerk erreicht haben.

1. Führen Sie `tracert/traceroute` mit einem bekannten Ziel wie z.B. `www.microsoft.com` aus. Wie viele Sprünge sind dazu erforderlich? Kommt es zu Zeitüberschreitungen oder kommen die Datenpakete problemlos durch?
2. Probieren Sie aus, mit `tracert/traceroute` die Route zu einem geografisch nahegelegenen Server zu verfolgen. Wenn es in der Nähe Ihres Wohnorts eine Universität gibt, können Sie die Route zu deren Webserver verfolgen. Sind hier weniger Sprünge erforderlich?

TCP/IP konfigurieren

Gemäß Voreinstellung ist das TCP/IP-Protokoll so konfiguriert, dass es eine IP-Adresse automatisch von einem DHCP-Server im Netzwerk bezieht (und eine entsprechende Subnetzmaske automatisch zuordnet). Soweit es die CompTIA A+-Zertifizierung betrifft, erhalten Sie die benötigten Informationen zu IP-Adresse, Subnetzmaske und Standardgateway von Netzwerktechnikern oder Administratoren. Sie konfigurieren den Rechner dann entsprechend. Viel mehr gibt es hierzu nicht, aber Sie sollen auch erfahren, wie die manuelle Einrichtung erfolgt.

1. Öffnen Sie in der Systemsteuerung das Applet NETZWERK- UND FREIGABECENTER und klicken Sie auf ADAPTEREINSTELLUNG ÄNDERN. Doppelklicken Sie anschließend das Symbol der gewünschten Netzwerkverbindung (meist LAN-VERBINDUNG oder WIFI).
2. Klicken Sie dann auf die Schaltfläche EIGENSCHAFTEN. Markieren Sie in der Liste die Option INTERNETPROTOKOLL VERSION 4 (TCP/IPV4). Klicken Sie erneut auf EIGENSCHAFTEN.
3. Im nun angezeigten Dialogfeld (Abbildung 19.13) aktivieren Sie die Option FOLGENDE IP-ADRESSE VERWENDEN.

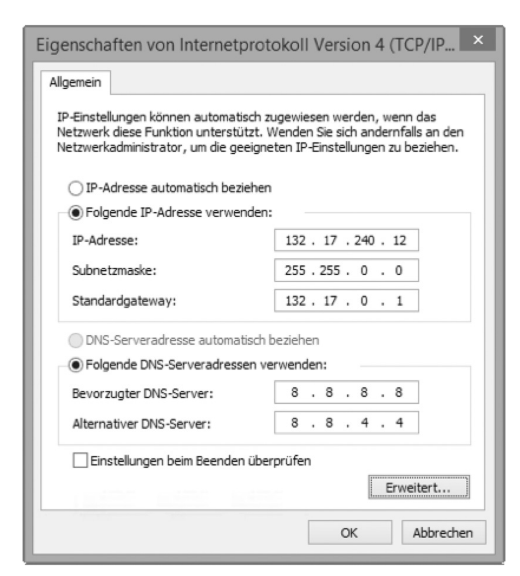


Abb. 19.13: TCP/IP-Einstellungen manuell festlegen

4. Geben Sie die IP-Adresse in die entsprechenden Felder ein.
5. Drücken Sie [Tab], um in das Feld SUBNETZMASKE zu wechseln. Beachten Sie, dass die Subnetzmaske automatisch eingetragen wird. (Sie können sie überschreiben, wenn Sie eine andere Subnetzmaske verwenden wollen.)

6. Optional können Sie die IP-Adressen eines Standardgateways angeben.
7. Optional können Sie die IP-Adresse eines primären oder sekundären DNS-Servers angeben. (In Abbildung 19.13 sind die Google-DNS-Server eingetragen.)
8. Klicken Sie jeweils die Schaltfläche OK an, um die Dialogfelder zu schließen.
9. Klicken Sie die Schaltfläche SCHLIESSEN an, um das Dialogfeld zu verlassen.

Automatische private IP-Adressierung

Moderne Betriebssysteme unterstützt eine Funktion namens *APIPA* in Windows (*Automatic Private IP Addressing*) bzw. *zeroconf* in anderen Betriebssystemen, die einem System auch dann automatisch eine IP-Adresse zuweist, wenn es sie nicht über einen DHCP-Server beziehen kann. Die *IANA* (*Internet Assigned Numbers Authority*), das für die Zuordnung von IP-Adressen und die Verwaltung von Rootservern zuständige nicht-kommerzielle Unternehmen, hat den Adressbereich von 169.254.0.1 bis 169.254.255.254 für diesen Zweck reserviert.

Wenn das Computersystem keine Verbindung zu einem DHCP-Server aufnehmen kann, dann erzeugt es eine Adresse nach dem Muster 169.254.x.y (bei x.y handelt es sich dabei um die Identifikation des Computers) und eine 16-Bit-Subnetzmaske (255.255.0.0) und fragt diese in seinem Netzwerksegment (Subnetz) ab. Wenn kein anderer Computer auf diese Adresse antwortet, dann weist es sich selbst diese Adresse zu. Wird APIPA verwendet, dann kann das System nur mit anderen Computern im selben Subnetz kommunizieren, die ebenfalls den Adressbereich 169.254.*x.y* mit einer 16-Bit-Maske nutzen. APIPA/zeroconf ist standardmäßig aktiviert, wenn das System für das automatische Beziehen von IP-Adressen konfiguriert wurde.

Hinweis

Wenn ein Computersystem in einem Netzwerk, in dem ein aktiver DHCP-Server vorhanden ist, eine IP-Adresse aus dem genannten Bereich verwendet, dann weist das darauf hin, dass Probleme bei der Verbindung mit dem DHCP-Server aufgetreten sind.

19.1.2 Netzwerk-Adressierung mit IPv6

Die Entwickler des frühen Internets sahen sich bei der Wahl einer Methode zur Adressierung oder Benennung von Geräten mehreren Problemen gegenüber. Natürlich musste dabei definiert werden, wie die Nummerierung oder die Namensgebung konkret funktioniert, und zu diesem Zweck wurden das Internetprotokoll und IP-Adressen erfunden. Aber darüber hinaus musste auch abgeschätzt werden, wie viele Computer es zukünftig geben wird, um den Adressraum dann noch deutlich größer auszulegen und bei der Namensgebung im Internet eine gewisse Langlebigkeit zu erzielen. Wie viele Computer würde es also zukünftig wohl geben?

Der 32-Bit-IPv4-Standard ermöglichte »nur« etwas mehr als 4 Milliarden Adressen. Das erschien damals viel zu sein, aber als sich das Internet global verbreitete, wurden allmählich die Adressen knapp.

Diese Entwicklung führte dazu, dass die *IETF* (*Internet Engineering Task Force*) eine neue Adressierungsmethode namens IPv6 (Internet Protocol version 6) entwickelte, die allmählich IPv4 ersetzt. Durch IPv6 wird der Adressraum von 32 Bit auf 128 Bit erweitert und kann so 2^{128} Adressen bereitstellen! Das sollte dieses Mal nun wirklich für die vorhersehbare Zukunft reichen! Die Anzahl der Adressen, etwa $3{,}4 \times 10^{38}$, entspricht ungefähr der Anzahl aller Sandkörner auf der Erde oder einem Achtel der Anzahl der Moleküle in der Erdatmosphäre.

Hinweis

Wenn Sie wirklich unbedingt wissen wollen, wie viele IPv6-Adressen es gibt, hier ist die Zahl: 340.282.366.920.938.463.463.374.607.431.768.211.456. Sagen Sie das drei Mal schnell hintereinander!

Auch wenn IPv6 und IPv4 demselben Zweck dienen, nämlich dem Versand von Datenpaketen in IP-Netzwerken, unterscheiden sich die Implementierungen der beiden Protokolle doch sehr. Dieser Abschnitt verschafft Ihnen einen schnellen Überblick über IPv6 und die Unterschiede zu IPv4.

Schreibweise von IPv6-Adressen

Die wohlbekannten IPv4-Adressen werden unter Verwendung von vier Oktetten als 197.169.94.82 notiert. Die Schreibweise der 128-Bit langen IPv6-Adressen sieht so aus:

```
2001:0000:0000:3210:0800:200c:00cf:1234
```

Als Trennzeichen wird statt eines Punktes, wie in der IPv4-Notation, bei IPv6 ein Doppelpunkt verwendet. Jede der »Vierergruppen« repräsentiert eine Hexadezimalzahl zwischen 0000 und ffff, die inoffiziell als *Feld* oder *Hextett* bezeichnet werden.

Wichtig

Die Buchstaben der Hexadezimalzahlen in IPv6-Adressen werden mal groß- und mal kleingeschrieben. Für den Computer spielt das keine Rolle, aber die hinter IPv6 stehenden Entwickler bestehen darauf (in RFC 5952), dass Kleinschreibung verwendet wird, deshalb verwende ich sie hier ebenfalls. Wundern Sie sich aber nicht, wenn in der Zertifizierungsprüfung die Großschreibung benutzt wird – sie bedeutet dasselbe.

Hinweis

Eine Hexadezimalzahl wie z.B. F/f repräsentiert 4 Bits, 4 Hexadezimalzahlen entsprechen somit 16 Bits. Aus unerfindlichen Gründen haben die IPv6-Entwickler diesen Vierergruppen keine Namen gegeben, sodass viele Techniker und Autoren sie einfach als »Feld« oder »Hextett« bezeichnen, auch um sie von den IPv4-Oktetten abzugrenzen.

Eine vollständige IPv6-Adresse besitzt acht Gruppen von jeweils vier Hexadezimalzahlen. Das hört sich so an, als ob Sie nun sehr lange IP-Adressen tippen müssten, aber keine Sorge, es gibt eine Reihe von Methoden, die schriftliche Form der Adressen zu verkürzen.

Führende Nullen jeder Gruppe dürfen entfallen Aus 00cf wird also cf und aus 0000 wird 0. Die vorige Adresse wird dadurch zu:

```
2001:0:0:3210:800:200c:cf:1234
```

Darüber hinaus dürfen Sie zusammenhängende Gruppen von Nullen entfernen, sodass dann zwei Doppelpunkte nebeneinanderstehen. Wenn Sie diese »::-Regel« beispielsweise auf

```
2001:0:0:3210:800:200c:cf:1234
```

anwenden, wird daraus

```
2001::3210:800:200c:cf:1234
```

Es darf zwar eine beliebig lange Gruppe zusammenhängender Nullen entfernt werden, allerdings nur ein einziges Mal. Sehen Sie sich die folgende IPv6-Adresse an:

```
fe80:0000:0000:0000:00cf:0000:ba98:1234
```

Hier gibt es vier Gruppen, die sich gemäß der ::-Regel entfernen ließen: Die ersten drei, die auf fedc folgen und eine weitere nach 00cf. Aufgrund der Einschränkung, die Regel nur einmalig anwenden zu dürfen, wäre es am vernünftigsten, die Adresse auf

```
fe80::cf:0:ba98:1234
```

zu verkürzen. Ein zweites »::«, um auch die vierte Gruppe von Nullen zu repräsentieren, ist nicht erlaubt. Es gibt einen guten Grund für diese Beschränkung: Angenommen, man würde mehr als ein »::« verwenden, wie soll man dann feststellen, wie viele Nullen in die verschiedenen Gruppen gehören? Antwort: Es ist unmöglich. Die Adresse ist dann nicht mehr eindeutig.

Wichtig

IPv4-Adressen verwenden 32 Bits und IPv6-Adressen 128 Bits. Diesen Unterschied und die Namenskonventionen sollten Sie kennen.

Hier ist ein schönes Beispiel einer speziellen IPv6-Adresse, die ausgiebigen Gebrauch von der ::-Regel macht, die IPv6-Loopback-Adresse: `::1`.

Ohne die Regel sähe diese IPv6-Adresse so aus:

```
0000:0000:0000:0000:0000:0000:0000:0001
```

Hinweis

Die unbestimmte Adresse (nur Nullen) darf nicht verwendet werden. Gleiches gilt für eine Adresse, die nur aus Einsen (binär) bzw. nur aus fs (hexadezimal) besteht.

In IPv6 werden weiterhin Subnetze verwendet, dabei wird für die Subnetzmaske jedoch die *CIDR-Nomenklatur* (*Classless Inter-Domain Routing*) verwendet, bei der nach einem Schrägstrich »/» die Anzahl der Bits in der Subnetzmaske wie bei IPv4 angegeben wird. Eine typische IPv6-Adresse eines Hosts mit Subnetzangabe sieht so aus:

```
fe80::cf:0:ba98:1234/64
```

Tipp

Sehen Sie sich die Übung zum Thema »IPv6-Adressen« im Abschnitt über Kapitel 19 unter `http://totalsem.com/100x` an. Sie können dadurch Ihre IPv6-Kenntnisse vertiefen.

Wie IPv6-Adressen bezogen werden

Bei IPv4 tippen Sie die IP-Adresse entweder selbst ein (statische IP-Adressierung) oder Sie verwenden DHCP (was auch als dynamische IP-Adressierung bezeichnet wird). Bei IPv6 funktioniert die Adressierung auf ganz andere Weise. Statt nur einer IP-Adresse können einer einzigen Netzwerkkarte mehrere IP-Adressen zugeordnet sein.

Wenn ein IPv6-Computer bootet, weist er sich selbst eine *verbindungslokale* oder *link-lokale Adresse* zu, dem IPv6-Pendant zur APIPA/zeroconf-Adresse von IPv4. Obwohl eine APIPA/zeroconf-Adresse einen Hinweis auf eine Netzwerkstörung oder ein Problem mit dem DHCP-Server darstellen kann, besitzen Computer, auf denen IPv6 läuft, stets eine verbindungslokale Adresse. Die ersten 64-Bits einer verbindungslokalen Adresse lauten immer `fe80::`. Jede dieser Adressen beginnt also mit `fe80:0000:0000:0000`. Falls Ihr System IPv6 unterstützt und es aktiv ist, können Sie sich diese

Adresse anzeigen lassen. In Abbildung 19.14 wird die link-lokale Adresse eines typischen Systems mithilfe des `ipconfig`-Hilfsprogramms angezeigt.

Wichtig

Alle Computer, auf denen IPv6 läuft, besitzen mindestens eine IPv6-Adresse: die verbindungslokale Adresse.

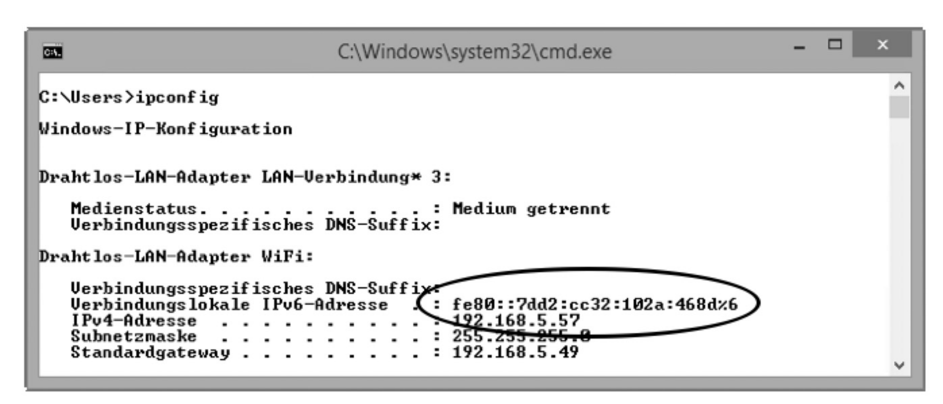


Abb. 19.14: Verbindungslokale IPv6-Adresse

Die letzten 64 Bits der IPv6-Adresse, die Interface-ID, wird auf zweierlei Weise gebildet. Aktuelle Betriebssysteme erzeugen eine 64-Bit-Zufallszahl. Sehr alte Betriebssysteme, wie Windows XP oder Windows Server 2003, nutzen eine alternative Methode, bei der die MAC-Adresse der Netzwerkkarte verwendet wird, die sogenannte *EUI-64* (*Extended Unique Identifier, 64-Bit*).

Die eigentliche Arbeit übernimmt bei IPv6 die link-lokale Adresse, und sofern Sie keine Internetverbindung benötigen, ist das schon ausreichend. Die alten Konzepte statischer IP-Adressen oder die Adressvergabe durch DHCP-Server ergeben bei IPv6 kaum einen Sinn, wenn man keine Server betreibt, denn auch bei IPv6 verfügen Server im Allgemeinen über eine statische IP-Adresse. Für das lokale Netzwerk sind link-lokale Adressen alles, was man braucht.

IPv6-Präfixlängen

Um festzustellen, ob Pakete an eine lokale MAC-Adresse oder über das Standardgateway ins Internet gesendet werden sollen, verwenden die Systeme die IPv6-Präfixlänge. Hier gibt es zwei neue Regeln:

- Die letzten 64 Bits einer IPv6-Adresse werden von der Netzwerkkarte generiert, sodass maximal 64 Bits für das Präfix verfügbar sind. Daher ist ein Präfix niemals länger als 64 Bits.
- Die fünf für die Verwaltung von IP-Adressen in einer Weltregion zuständigen Regional Internet Registries (RIRs) teilt großen Internetanbietern und Organisationen, die umfangreiche Kontingente benötigen, /48-Präfixe zu. Die Internetanbieter ihrerseits vergeben /64-Präfixe an Endkunden. Die linklokale Adressierung verwendet eine Präfixlänge von /64. Andere Arten von IPv6-Adressen erhalten die Subnetzinformationen automatisch vom Router.

Globale Unicast-Adressen

Zur Verbindung mit dem Internet benötigt ein System eine zweite IPv6-Adresse, die *globale Unicast-Adresse* genannt wird. Für gewöhnlich weist der Standardgateway-Router, der für die Vergabe globaler IPv6-Adressen konfiguriert sein muss, dem Rechner diese zu. Wenn Sie einen Rechner mit einem Netzwerk verbinden, versendet er auf der Suche nach einem Router ein spezielles Paket (*router solicitation* oder kurz *RS*, siehe Abbildung 19.15). Der Router erkennt diese Nachricht und antwortet mit

einem *router advertisement* (*RA*), das dem Rechner die Netzwerk-ID, das Subnetz (die zusammen als *Präfix* bezeichnet werden) und gegebenenfalls den DNS-Server mitteilt.

Hinweis

Für die RS-Nachricht wird die Adresse ff02::2 verwendet, die nur von denjenigen Rechnern des Netzwerks erkannt wird, auf denen ebenfalls IPv6 läuft. Diese Adressart unterscheidet sich von Broadcast-Adressen und wird als Multicast-Adresse bezeichnet. Bei IPv6 gibt es keine Broadcast-Adresse, sondern nur Multicast.



Abb. 19.15: Bezug einer globalen Adresse

Sobald dem Computer das Präfix zugewiesen wurde, erzeugt er den Rest der Adresse – ebenso wie bei link-lokalen Adressen – selbst. Der Computer besitzt nun neben seiner link-lokalen Adresse eine gültige, öffentliche 128-Bit-IPv6-Adresse. Abbildung 19.16 zeigt die IPv6-Informationen in macOS.

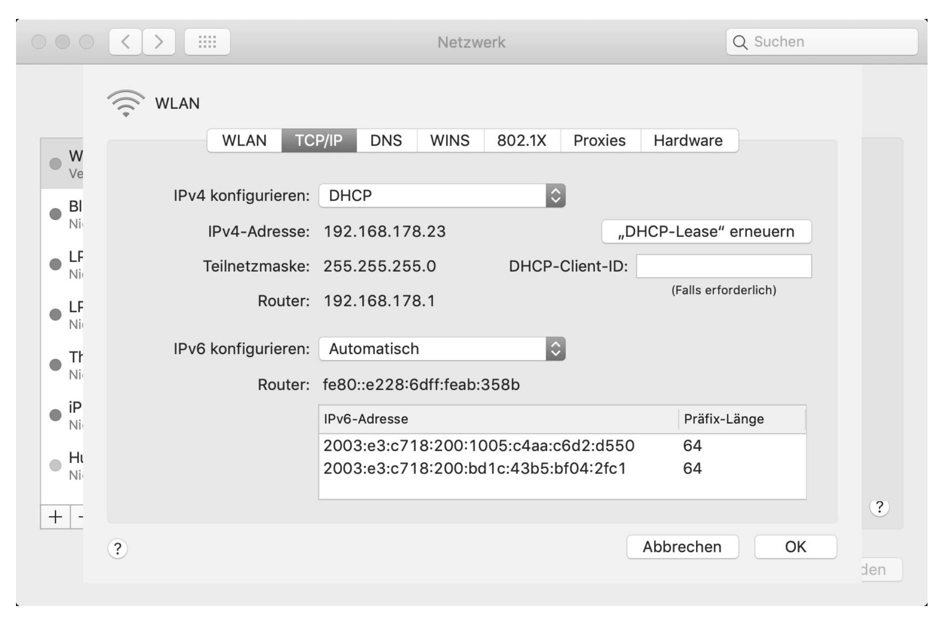


Abb. 19.16: macOS-System mit globaler IPv6-Adresse

Globale Adressen sind vollwertige Internetadressen, sodass ein anderer IPv6-Computer mit gültiger IPv6-Adresse auf Ihr System zugreifen kann, sofern nicht irgendeine Art von Firewall das verhindert.

Wichtig

Für den Zugriff aufs Internet ist eine globale Unicast-IPv6-Adresse erforderlich.

Durch die Unterstützung von IPv6 werden Hilfsprogramme wie `ipconfig` ziemlich kompliziert. Werfen Sie nur einmal einen Blick auf Abbildung 19.17.

```
Eingabeaufforderung
Drahtlos-LAN-Adapter WiFi:

   Verbindungsspezifisches DNS-Suffix: fritz.box
   Beschreibung. . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3160
   Physische Adresse . . . . . . . . : A0-88-69-A6-38-80
   DHCP aktiviert. . . . . . . . . . : Ja
   Autokonfiguration aktiviert . . . : Ja
   IPv6-Adresse. . . . . . . . . . . : 2003:e3:c718:200:7dd2:cc32:102a:468d(Bevorzugt)

   Temporäre IPv6-Adresse. . . . . . : 2003:e3:c718:200:d820:dcec:3fe0:7835(Bevorzugt)

   Verbindungslokale IPv6-Adresse  . : fe80::7dd2:cc32:102a:468d%7(Bevorzugt)
   IPv4-Adresse  . . . . . . . . . . : 192.168.178.24(Bevorzugt)
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Lease erhalten. . . . . . . . . . : Mittwoch, 23. Oktober 2019 20:09:21
   Lease läuft ab. . . . . . . . . . : Sonntag, 3. November 2019 15:08:17
   Standardgateway . . . . . . . . . : fe80::e228:6dff:feab:358b%7
                                       192.168.178.1
   DHCP-Server . . . . . . . . . . . : 192.168.178.1
   DHCPv6-IAID . . . . . . . . . . . : 161515625
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-1E-4F-D3-13-7C-D3-0A-00-19-AC
   DNS-Server  . . . . . . . . . . . : fd00::e228:6dff:feab:358b
                                       192.168.178.1
                                       fd00::e228:6dff:feab:358b
   NetBIOS über TCP/IP . . . . . . . : Aktiviert

C:\Users>
```

Abb. 19.17: `ipconfig` bei Verwendung von IPv4 und IPv6

19.2 Installation und Konfiguration eines kabelgebundenen Netzwerks

Damit die Netzwerkverbindungen funktionieren, müssen die folgenden Dinge gegeben sein:

- **Verbundener Netzwerkadapter (NIC)**: Dabei handelt es sich um die physische Hardware, die für die Verbindung des Rechnersystems mit dem Netzwerkkabel sorgt.
- **Korrekt konfigurierte IP-Adressierung**: Ihr Rechner benötigt die für Ihr Netzwerk passende IP-Adressierung.
- **Switch**: In einem kabelgebundenen Netzwerk sind alle Geräte mit dem Switch verbunden.

Wenn Sie Ressourcen auf dem lokalen Rechner für andere Netzwerkbenutzer freigeben wollen, dann müssen Sie auch die Datei- und Druckerfreigabe aktivieren. Wenn Sie einen Netzwerkadapter einrichten, dann installiert Windows bei dessen Einrichtung standardmäßig das TCP/IP-Protokoll, den Client für Microsoft-Netzwerke und die Datei- und Druckerfreigabe für Microsoft-Netzwerke. Computer mit macOS sind ab Werk vollständig für die Nutzung von Netzwerken eingerichtet und die verschiedenen Linux-Distributionen bieten ähnliche Möglichkeiten wie Windows.

19.2.1 Installation einer Netzwerkkarte

Die Netzwerkkarte sorgt für die Verbindung des Rechnersystems mit dem Netzwerk, weshalb sie zunächst installiert werden muss, wenn eine Verbindung zu einem Netzwerk hergestellt werden soll. Das war lange für die Zertifizierungsprüfung von großer Bedeutung und Fragen dazu könnten vorkommen, aber inzwischen ist in allen modernen Computern eine Gigabit-Netzwerkkarte integriert. Windows installiert bei der Einrichtung automatisch einen Treiber für die Netzwerkkarte.

Vollduplex und Halbduplex

Alle aktuellen Netzwerkkarten beherrschen den Vollduplex-Modus, das heißt, sie können gleichzeitig Daten senden und empfangen. Die meisten Netzwerkkarten und Switches bieten eine Funktion namens *Autosensing*, um sehr alte mit dem Netzwerk verbundene Geräte zu unterstützen, die nur den Halbduplex-Modus beherrschen. Halbduplex bedeutet, dass das Gerät zwar sowohl senden als auch empfangen kann, jedoch nicht gleichzeitig. Wenn Sie die Duplex-Einstellung oder die Geschwindigkeit einer Netzwerkkarte ändern möchten, öffnen Sie ihr Dialogfeld EIGENSCHAFTEN, klicken Sie auf KONFIGURIEREN, um das entsprechende Dialogfeld zu öffnen, und wählen Sie die Registerkarte ERWEITERT. Wählen Sie in der Liste auf der linken Seite SPEED & DUPLEX aus und passen Sie den Wert auf der rechten Seite an das alte Gerät an, das Schwierigkeiten bereitet (Abbildung 19.18).

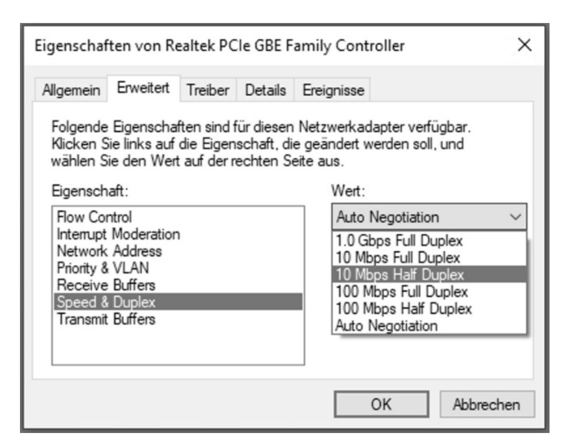


Abb. 19.18: Anpassung der Einstellungen einer Netzwerkkarte in Windows 10

Statusanzeigen

Die heutzutage hergestellten Netzwerkkarten besitzen LEDs zur *Statusanzeige*, die über den Zustand der Netzwerkverbindung Auskunft erteilen. Es gibt Netzwerkkarten mit bis zu vier Status-LEDs verschiedener Farbe. Die LEDs geben Hinweise darauf, was bei der Netzwerkverbindung gerade vor sich geht, und sollten als Erstes überprüft werden, wenn Sie glauben, dass ein Gerät seine Netzwerkverbindung verloren hat (Abbildung 19.19).

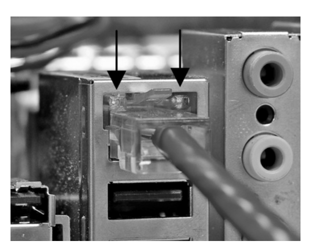


Abb. 19.19: So schön bunt hier!

Auch Switches besitzen derartige LEDs, die den Verbindungszustand der angeschlossenen Kabel anzeigen. Überprüfen Sie zuerst diese Anzeige, wenn ein PC keine Netzwerkverbindung herstellen kann. Switches, die verschiedene Geschwindigkeiten unterstützen, zeigen für gewöhnlich an, welche Verbindungsgeschwindigkeit bei einem Anschluss aktiv ist. In Abbildung 19.20 ist beispielsweise die LED für Port 2 im oberen Foto orange und zeigt dadurch an, dass das angeschlossene Kabel mit einer 10BaseT- oder 100BaseT-Netzwerkkarte verbunden ist. Wenn derselbe Port mit einer Gigabit-Netzwerkkarte verbunden ist, leuchtet die LED hingegen grün (unteres Bild).



Abb. 19.20: Farbige LEDs zur Geschwindigkeitsanzeige

Eine LED zur Anzeige des *Verbindungsstatus* leuchtet konstant, sofern die Verbindung ordnungsgemäß funktioniert. Kein Flackern, kein An und Aus, sie leuchtet einfach nur. Blinkt oder flackert sie hingegen, deutet das auf ein Verbindungsproblem hin.

Bei einer LED zur *Aktivitätsanzeige* verhält es sich anders. Diese blinkt, wenn Datenverkehr festgestellt wird. Die Aktivitätsanzeige ist ungemein hilfreich, wenn es darum geht, Probleme aufzuspüren, weil die LEDs zur Verbindungsanzeige im wahren Leben manchmal nicht den tatsächlichen Zustand einer Verbindung wiedergeben. Wenn die Verbindung gemäß der Verbindungsstatusanzeige in Ordnung ist, sollten Sie eine Datei kopieren oder auf andere Art Datenverkehr erzeugen. Blinkt die Aktivitätsanzeige dann nicht, liegt ein Problem vor.

Für die verschiedenen Status-LEDs gibt es keinen einheitlichen Standard, daher gibt es diese Statusanzeigen in allen möglichen Formen und Farben. Nehmen Sie sich bei Ihnen unbekannten Netzwerkkarten einen Moment Zeit, um herauszufinden, was die einzelnen LEDs bedeuten. Auch wenn es diese LEDs in den verschiedensten Ausführungen gibt, zeigen sie letztlich doch immer dasselbe an: Verbindungsstatus, Geschwindigkeit und Aktivität.

Wichtig

Es gibt zwar keinen Standard für die LED-Anzeigen von Netzwerkkarten, dennoch kommen in den CompTIA A+-Prüfungen Fragen nach der in der Praxis gängigen Bedeutung der LEDs vor. Sie sollten wissen, dass konstant grünes Licht eine Verbindung anzeigt, blinkendes grünes Licht eine zeitweise Verbindung und fehlendes grünes Licht keine Verbindung bedeutet. Blinkende bernsteinfarbene LEDs weisen auf Netzwerkkollisionen hin (was in manchen Fällen durchaus in Ordnung sein kann). Sie sollten außerdem wissen, dass der erste Schritt bei der Fehlersuche im Fall von Verbindungsstörungen die Überprüfung der Netzwerkkarten-LEDs ist.

Wake-on-LAN

Viele Netzwerkkarten sind dazu in der Lage, einen abgeschalteten oder im Ruhezustand befindlichen Computer einzuschalten oder aufzuwecken. In Kapitel 23 wird die Energieverwaltung ausführlich vorgestellt, aber an dieser Stelle sollten Sie bereits zur Kenntnis nehmen, dass *Wake-on-LAN* wirklich praktisch ist, wenn Sie einen oder mehrere Computer aufwecken möchten, die physisch weit von Ihnen entfernt sind. Dazu senden Sie an die betroffenen PCs ein spezielles Datenpaket oder ein sogenanntes *magisches Paket*. (Dabei handelt es sich um ein Broadcast-Paket, das im Wesentlichen die MAC-Adresse des Zielrechners mehrmals wiederholt.)

Ein abgeschalteter oder im Ruhezustand befindlicher Rechner erkennt dieses spezielle Muster bzw. Paket, sofern er dafür eingerichtet wurde. Öffnen Sie dazu unter Windows das NETZWERK- UND FREIGABECENTER und klicken Sie links auf ADAPTEREINSTELLUNGEN ÄNDERN. Klicken Sie dann mit der rechten Maustaste auf den Netzwerkadapter und wählen Sie EIGENSCHAFTEN aus. Klicken Sie auf KONFIGURIEREN und wählen Sie die Registerkarte ENERGIEVERWALTUNG aus (Abbildung 19.21). Zum Aktivieren von Wake-on-LAN müssen Sie das Kontrollkästchen neben GERÄT KANN DEN COMPUTER AUS DEM RUHEZUSTAND AKTIVIEREN markieren. Optional können Sie auch NUR MAGIC PACKET KANN COMPUTER AUS DEM RUHEZUSTAND AKTIVIEREN markieren, um die Netzwerkkarte anzuweisen, mit Ausnahme von magischen Paketen sämtlichen Datenverkehr zu ignorieren.



Abb. 19.21: Wake-on-LAN-Einstellungen

> **Hinweis**
>
> Möglicherweise gibt es auch im BIOS Einstellungen zur Steuerung von Wake-on-LAN. Verwenden Sie das CMOS-Setup, um dies zu überprüfen.

Wake-on-LAN ist sehr bequem, hat aber einen ärgerlichen Nachteil. Wie dem EIGENSCHAFTEN-Dialogfeld zu entnehmen ist, lassen sich Laptops per Wake-on-LAN mittels drahtloser Netzwerkverbindung einschalten oder aufwecken, sogar wenn diese nicht an der Stromversorgung angeschlossen sind oder sich in einer Tragetasche befinden. Dabei kann die Batterie Schaden nehmen oder überhitzen. Wenn Sie nicht genau wissen, dass Sie die Funktion benötigen, sollten Sie bei Laptops Wake-on-LAN abschalten.

QoS

QoS (*Quality of Service*, Dienstgüte) ermöglicht es in stark ausgelasteten Netzwerken, bestimmten Datenverkehr zu priorisieren. In Kapitel 21, *Das Internet*, betrachten wir QoS aus Sicht des Routers. Die einzelnen Systeme spielen aber auch eine wichtige Rolle, da sie die Frames kennzeichnen müssen, damit die Geräte im Netzwerk sie entsprechend der vom Netzwerkadministrator festgelegten Regeln behandeln. Die Unterstützung von QoS ist bei den meisten Netzwerkadaptern standardmäßig aktiviert. Falls Sie diese Einstellung ändern möchten, finden Sie die Option PRIORITÄT & VLAN auf der Registerkarte ERWEITERT im EIGENSCHAFTEN-Dialogfeld der Netzwerkkarte (Abbildung 19.22).

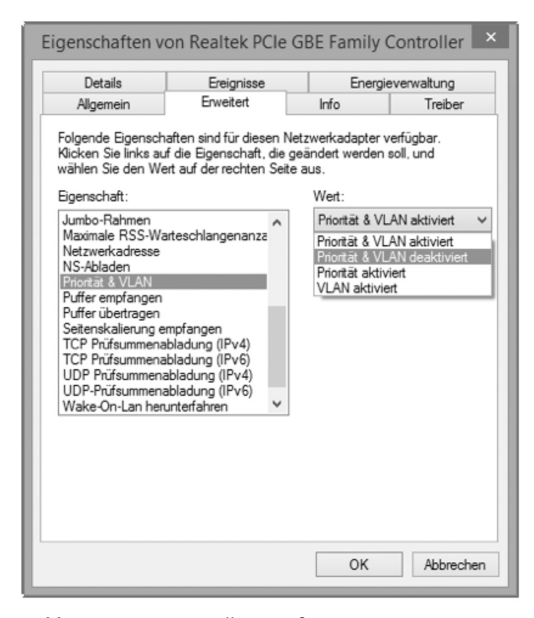


Abb. 19.22: Die Einstellungen für PRIORITÄT UND VLAN

19.2.2 Konfiguration der IP-Adressierung

Alle Betriebssysteme sind standardmäßig für die Verwendung von DHCP vorkonfiguriert und erhalten die Adresseinstellungen automatisch. Das gilt sowohl für IPv4 als auch für IPv6. Und wenn Sie tatsächlich doch einmal einen so konfigurieren müssen, dass er eine statische IP-Adrese verwendet, ist das problemlos möglich.

19.2.3 Verbindung mit einem Switch

Alle Computer in einem kabelgebundenen Netzwerk sind mit einem Switch verbunden, der es ermöglicht, mit anderen Rechnern im Netzwerk zu kommunizieren. Es gibt Switches mit Management-Funktionen und solche ohne. Plug-and-Play-Switches kommunizieren anhand der MAC-Adressen und müssen nicht konfiguriert werden. Sie leisten allerdings auch kaum mehr, als die Geräte miteinander zu verbinden.

Ein Switch mit Management-Funktionen bietet viele zusätzliche Features, die moderne Netzwerke versenden, um effizienter und sicherer zu funktionieren. Er besitzt eine eigene IP-Adresse, die Sie dazu verenden können, weitere Optionen zu konfigurieren. Abbildung 19.23 zeigt die Bedienoberfläche eines Switches mit Management-Funktionen. Die Handhabung von Switches gehört eigentlich zu den Themenbereichen CompTIA Netzwerk+ und CompTIA Sicherheit+, aber wenn Sie in eine Situation

geraten, in der Sie auf solch einen Switch zugreifen müssen, sollten Sie wissen, dass zu diesem Zweck die IP-Adresse und eine Netzwerkanwendung verwendet werden.

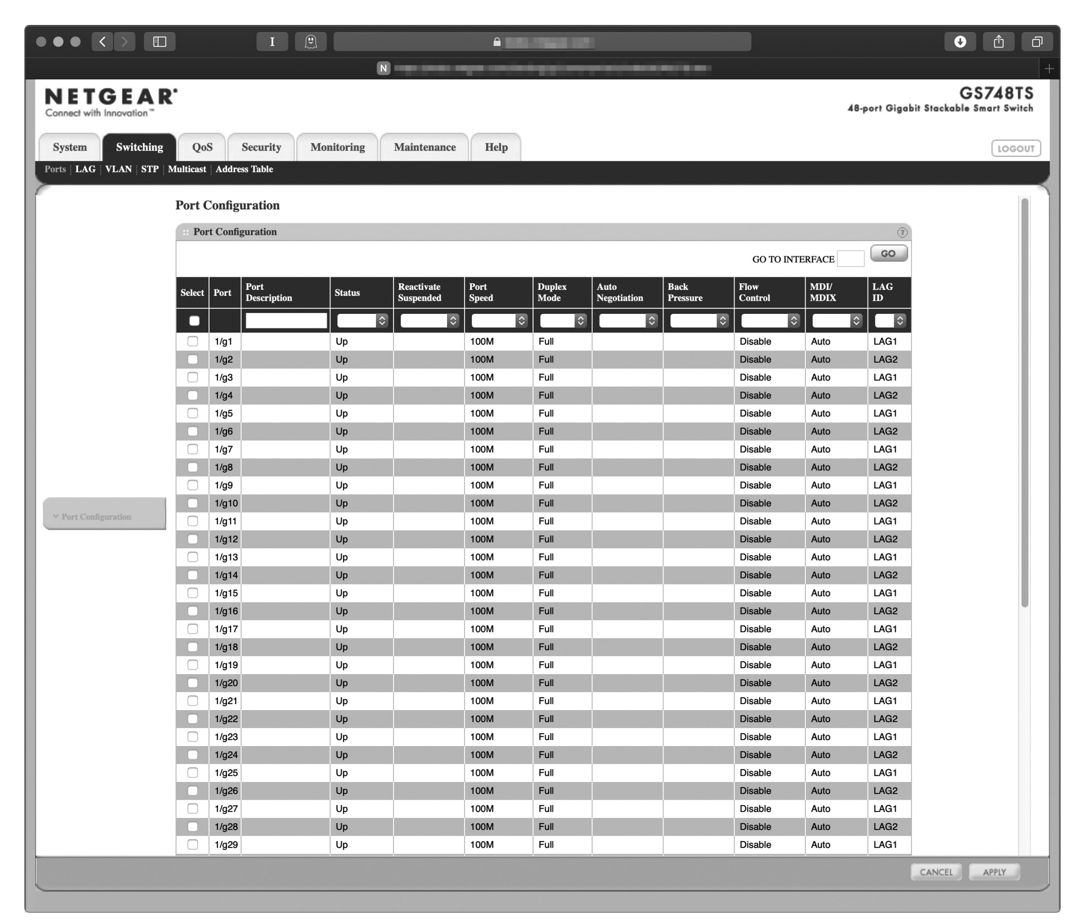


Abb. 19.23: Bedienoberfläche eines Switches mit Management-Funktionen

Hinweis

Ich kehre hier die Komplexität, die Switches mit Management-Funktionen mit sich bringen können, unter den Teppich. Manche Switches verfügen über eine einfache IP-basierte Bedienoberfläche wie die in Abbildung 19.23. Andere werden mittels einer speziellen Software über das Netzwerk verwaltet. Hier gibt es eine große Vielfalt.

VLANs sind ein schönes Beispiel für die Leistungsfähigkeit von Switches mit Management-Funktionen. Sie können ein einzelnes physisches Netzwerk *segmentieren*, also in mehrere getrennte Teilnetzwerke (Segmente) aufteilen. Alle in einem VLAN (*Virtual Local Area Network*) befindlichen Computer können miteinander kommunizieren, nicht aber mit Computern in einem anderen VLAN. Und jetzt wird es interessant: Wenn an einem einzelnen Switch beispielsweise 24 Computer angeschlossen sind, würden alle 24 normalerweise zum gleichen Netzwerk gehören. Bei einem VLAN-fähigen Switch können Sie jedoch die physischen Anschlüsse des Switches verschiedenen VLANs zuordnen. Sie könnten beispielsweise die Anschlüsse 1 bis 12 einem VLAN100 und die Anschlüsse 13 bis 24 einem

VLAN200 zuweisen. Mit dem Anschluss 12 bzw. 13 verbundene Computer könnten den jeweils anderen Rechner überhaupt nicht erkennen. Eine ausführliche Erläuterung von VLANs und was man mit ihnen alles anstellen kann, hebe ich mir für das nächste CompTIA Network+-Buch auf.

19.2.4 Ressourcenfreigabe und Sicherheit

Windows-Systeme können alle möglichen Ressourcen freigeben: Dateien, Ordner, komplette Laufwerke, Drucker, Faxgeräte, Internetverbindungen und noch viel mehr. Wie praktisch (für Sie), dass sich das Interesse der CompTIA A+-Zertifizierungsprüfungen auf Ordner, Drucker, Multifunktionsgeräte und Internetverbindungen beschränkt. Hier werden wir uns zunächst mit der Freigabe von Ordnern und Druckern befassen. Multifunktionsgeräte kommen in Kapitel 26, *Drucker und Multifunktionsgeräte*, an die Reihe und die Freigabe von Internetverbindungen hebe ich mir für Kapitel 21, *Das Internet*, auf.

19.2.5 Freigabe von Laufwerken und Ordnern

Wenn Sie Ordner und Laufwerke freigeben, verwenden alle Betriebssysteme bestimmte Berechtigungen, um Zugriff auf gemeinsam genutzte Ressourcen zu gewähren oder zu verweigern. Diese Berechtigungen haben jedoch nichts mit den auf Datei- oder Ordnerebene vergebenen Berechtigungen des NTFS-Dateisystems zu tun, das Ihnen bereits aus Kapitel 13, *Benutzer, Gruppen und Berechtigungen*, bekannt ist. Die NTFS-Berechtigungen haben aber dennoch einen Einfluss auf die für Netzwerkfreigaben geltenden Berechtigungen. Es folgen die Einzelheiten.

Auf Laufwerken ohne NTFS, wie optischen Medien oder USB-Speichersticks, gibt es nur drei Berechtigungsebenen: Lesen, Lesen/Schreiben und Besitzer. (Auf diese Berechtigungen komme ich später noch einmal zurück.) Bei erweiterten Freigaben heißen diese Berechtigungsebenen Lesen, Ändern und Vollzugriff.

Wenn Sie einen Ordner auf einem NTFS-Laufwerk freigeben, wie dies heute normalerweise üblich ist, dann müssen Sie *sowohl* die Netzwerkberechtigungen *als auch* die NTFS-Berechtigungen konfigurieren, damit andere Anwender auf die freigegebenen Ressourcen zugreifen können. Die Freigabe stellt die fragliche Ressource zwar über das Netzwerk bereit, aber NTFS legt fest, was die Benutzer überhaupt damit anfangen können.

Die gute Nachricht lautet aber: Eigentlich ist das gar nicht weiter problematisch! Stellen Sie die Netzwerkberechtigungen einfach so ein, dass alle Benutzer Vollzugriff haben, und nutzen Sie dann die NTFS-Berechtigungen, um festzulegen, *wer* auf die freigegebenen Ressourcen zugreifen darf und *wie* darauf zugegriffen werden darf. Um die NTFS-Berechtigungen einzustellen, aktivieren Sie die Registerkarte SICHERHEIT. Wir sehen uns das im nächsten Abschnitt genauer an.

Wichtig

Den Unterschied zwischen Netzwerkberechtigungen und NTFS-Berechtigungen sollten Sie kennen. Netzwerkberechtigungen betreffen nur die Freigabe im Netzwerk. NTFS-Berechtigungen gelten sowohl für lokale Ressourcen als auch für Netzwerkfreigaben.

19.2.6 Organisation des Netzwerks

Sobald ein Netzwerk eingerichtet ist, möchten die Benutzer Ressourcen miteinander teilen, und zwar auf vernünftig organisierte Art und Weise. Betriebssysteme müssen irgendwie feststellen können, wer freigegebene Ordner und Drucker verwenden darf (und wer nicht) und in welcher Form. Microsoft stellt zu diesem Zweck drei Kategorien von Windows-Netzwerken bereit: Arbeitsgruppen, Domänen und Heimnetzgruppen. (Hierbei handelt es sich um Microsoft-Terminologie, aber vergleichbare Konzepte finden in der gesamten Computerbranche Anwendung und betreffen macOS und andere Betriebssysteme ebenso.) Diese drei Kategorien unterscheiden sich hinsichtlich Verwaltung, Anzahl der erforderlichen Computer, Kompatibilität und Sicherheitsaspekten.

Nehmen wir zunächst die älteste Organisationsform in Augenschein: Arbeitsgruppen.

Arbeitsgruppen

Die *Arbeitsgruppe* ist die grundlegendste und einfachste Form der Zusammenarbeit im Netzwerk und gleichzeitig der Standard bei nahezu allen neu installierten Windows-Versionen.

Standardmäßig wird jeder Computer im Netzwerk einer Arbeitsgruppe mit der Bezeichnung WORKGROUP zugeordnet. Sie können den Namen Ihrer Arbeitsgruppe anzeigen, indem Sie das Applet SYSTEM aufrufen (Abbildung 19.24).

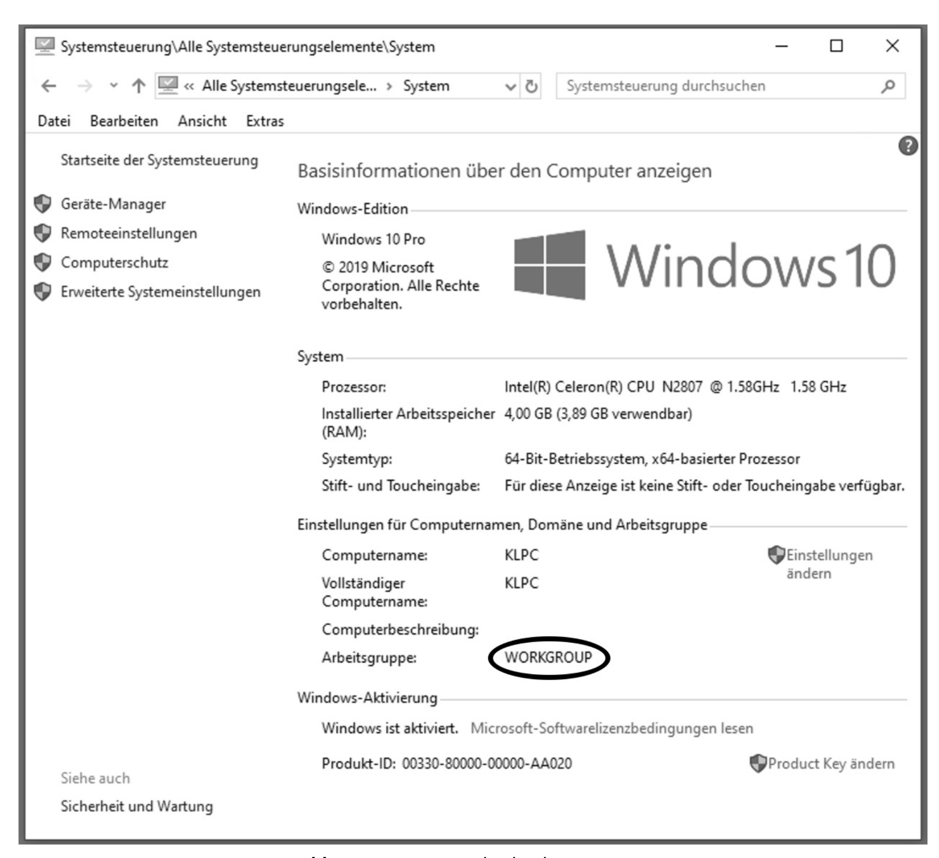


Abb. 19.24: Die Standard-Arbeitsgruppe

Am Namen WORKGROUP gibt es nichts Besonderes außer der Tatsache, dass jeder Computer im Netzwerk dieselbe Bezeichnung verwenden muss, um Ressourcen freigeben zu können. Wenn Sie den Namen Ihrer Arbeitsgruppe ändern möchten, können Sie dazu das Applet SYSTEM verwenden. Klicken Sie auf EINSTELLUNGEN ÄNDERN, um das Dialogfeld SYSTEMEIGENSCHAFTEN anzuzeigen. Klicken Sie dann auf ÄNDERN, um den Namen Ihrer Arbeitsgruppe zu ändern (Abbildung 19.25).

Hinweis

Wenn Sie den Namen der Arbeitsgruppe eines Systems ändern, müssen Sie ihn auch bei allen anderen Geräten ändern, die zu dieser Arbeitsgruppe gehören sollen.

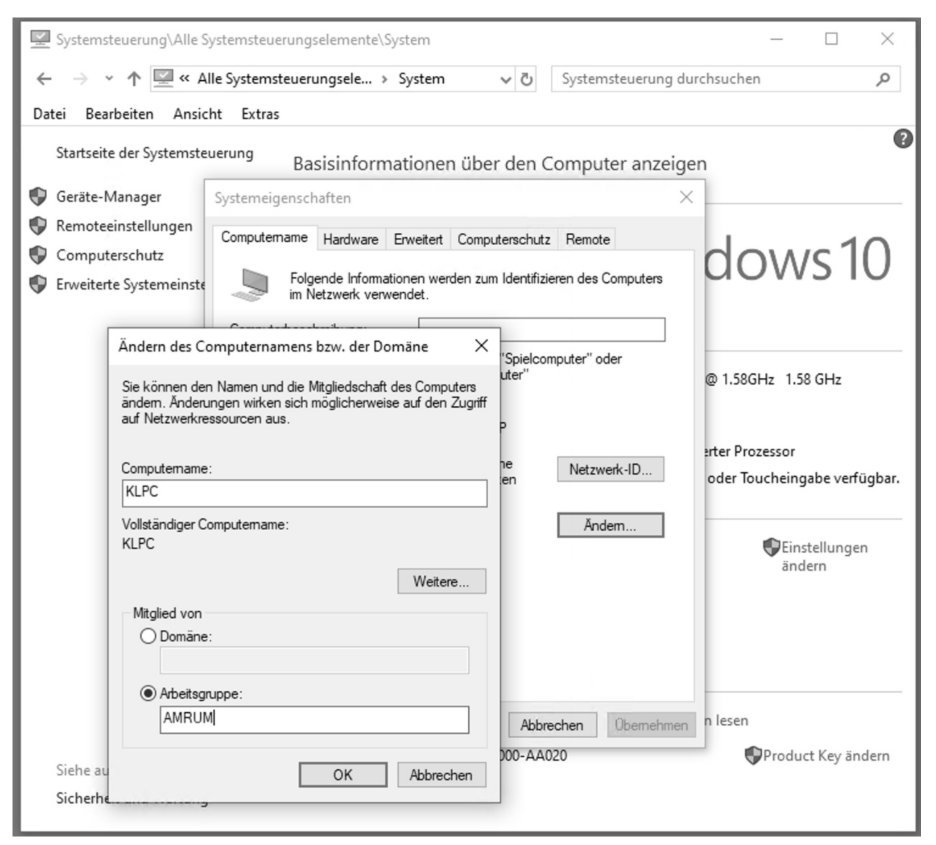


Abb. 19.25: Ändern des Namens der Arbeitsgruppe

In macOS können Sie den Namen der Arbeitsgruppe unter SYSTEMEINSTELLUNGEN|NETZWERK ändern. Klicken Sie auf WEITERE OPTIONEN ... und wählen Sie die Registerkarte WINS aus.

Hinweis

Um Linux-Rechner zu einer Windows-Arbeitsgruppe hinzuzufügen, müssen sowohl auf den Windows-Rechnern als auch auf den Linux-Computern erheblich mehr manuelle Konfigurationen vorgenommen werden. Im Internet finden sich zahlreiche schrittweise Anleitungen, falls Sie daran interessiert sind.

Bei Arbeitsgruppen gibt es keine zentrale Kontrolle des Netzwerks; alle mit dem Netzwerk verbundenen Systeme sind gleichwertig. Am besten funktioniert das mit kleinen Netzwerken, da es hier nur wenige Benutzer, Verbindungen und zu berücksichtigende Sicherheitsaspekte gibt. Wenn Ihr Netzwerk nun aber Hunderte von Benutzern und Systemen umfasst? Wie kann man das Ganze unter Kontrolle bringen?

Benutzernamen und Kennwörter Wie Sie aus Kapitel 13 bereits wissen, müssen Sie bei der Windows-Anmeldung einen Benutzernamen und ein Kennwort eingeben. Windows vereinfacht diesen Vorgang, indem es Ihnen eine schicke Schnittstelle zum Anmelden präsentiert (Abbildung 19.26). Die Angabe eines Benutzernamens stellt eine *Identifizierung* dar; die Eingabe eines Kennworts ist eine *Authentifizierung*, also der Vorgang, der es dem System ermöglicht, einem Benutzer Zugriff auf Ressourcen zu gewähren.

Hinweis

Der Unterschied zwischen Identifizierung und Authentifizierung ist für die CompTIA A+-Zertifizierung nicht von Belang, spielt aber bei Netzwerk+ und Sicherheit+ eine Rolle. Merken Sie ihn sich besser schon jetzt!

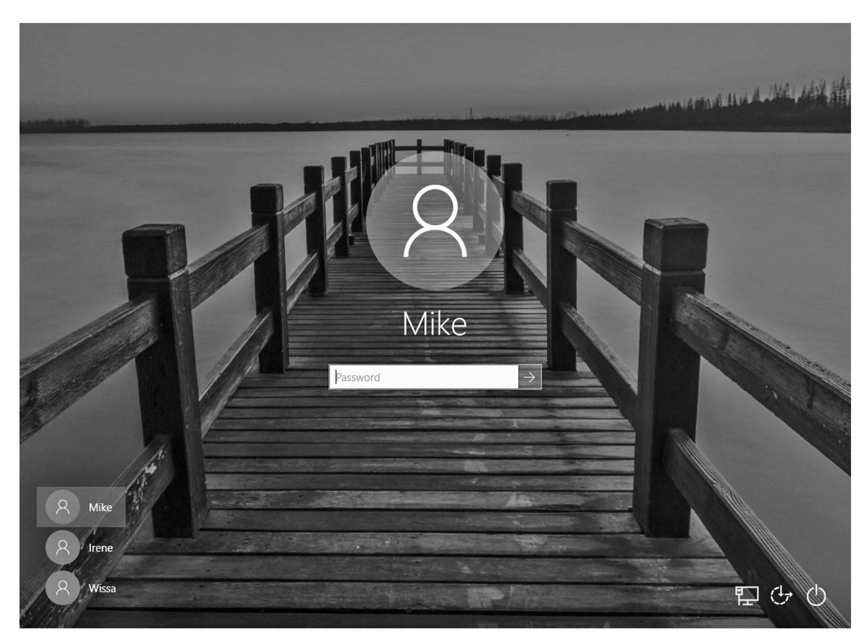


Abb. 19.26: Der Anmeldebildschirm von Windows

Benutzernamen und die dazugehörigen Kennwörter werden auf Ihrem Computer in verschlüsselter Form abgespeichert. Die Benutzernamen werden auf Ihrem Computer für eine Reihe verschiedener Aufgaben benutzt, aber hier sind wir vor allem daran interessiert, dass ein Benutzer Zugriff auf den Computer erhält. Für den Zugriff auf Ihren eigenen Computer sind Benutzernamen gut geeignet, aber dieselben Benutzernamen und Kennwörter finden auch beim Zugriff auf geteilte Ressourcen anderer Computer im Netzwerk Verwendung – und hier beginnt es, problematisch zu werden. Um uns dieser Problematik bewusst zu werden, betrachten wir nun, wie eine typische Ordnerfreigabe in einem Netzwerk mit Windows-Systemen vonstattengeht.

Dateifreigaben Alle Computer unterstützen von Haus aus Ordner- und Druckerfreigaben. Es ist ganz einfach, in Windows einen Ordner freizugeben. Klicken Sie mit der rechten Maustaste auf einen Ordner und wählen Sie FREIGEBEN FÜR|BESTIMMTE PERSONEN (in Windows 7) oder ZUGRIFF GEWÄHREN AUF|BESTIMMTE PERSONEN (Windows 8/8.1/10) im Kontextmenü aus, um das Dialogfeld PERSONEN FÜR DIE FREIGABE AUSWÄHLEN anzuzeigen (Abbildung 19.27).

Standardmäßig werden Ihnen alle Benutzerkonten angezeigt, die aktuell auf dem System vorhanden sind. Sie können einem Benutzerkonto Lese- oder Schreib-/Leserechte zuweisen. Derjenige Benutzer, der den Ordner angelegt hat, ist dessen Besitzer. Die Zugriffsrechte sind dann die Folgenden:

- **Lesen**: Sie dürfen den Inhalt des Ordners anzeigen und darin befindliche Dateien öffnen, jedoch nicht wieder in dem Ordner abspeichern.
- **Schreiben/Lesen**: Wie bei Lesen, allerdings ist das Abspeichern im Ordner erlaubt.
- **Besitzer**: Wie bei Schreiben/Lesen, außerdem dürfen Sie die Zugriffsberechtigungen der anderen Benutzer für den Ordner vergeben.

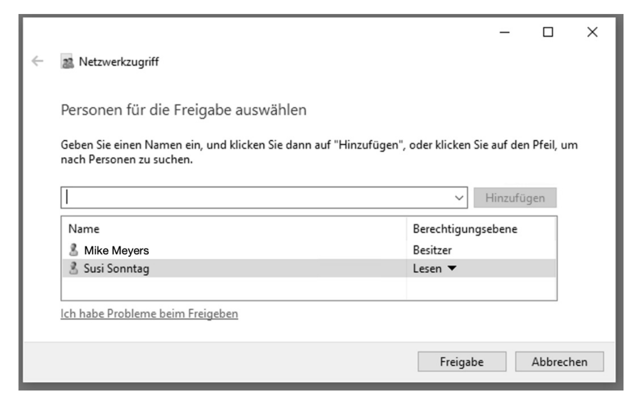


Abb. 19.27: Ordnerfreigabe in Windows 10

Hinweis

Wie Sie aus Kapitel 13 wissen, gibt es in Windows eine sehr viel leistungsfähigere und kompliziertere Art von Zugriffsberechtigungen, die auf dem NTFS-Dateisystem beruht.

Erweiterte Freigabe Die erweiterte Freigabe ermöglicht es, Netzwerkfreigaben zu erstellen, bei denen Sie den Zugriff auf die Inhalte sehr viel genauer steuern können. (In der Praxis neigen Techniker allerdings dazu, alle Berechtigungen auf Vollzugriff zu setzen und die Autorisierung auf lokaler Ebene NTFS zu überlasen.) Klicken Sie mit der rechten Maustaste auf den freizugebenden Ordner, wählen Sie EIGENSCHAFTEN aus und begeben Sie sich zur Registerkarte FREIGABE. Abbildung 19.28 zeigt die Registerkarte FREIGABE eines Ordners namens MUSIK, der `.mp3`- und `.aac`-Dateien enthält.

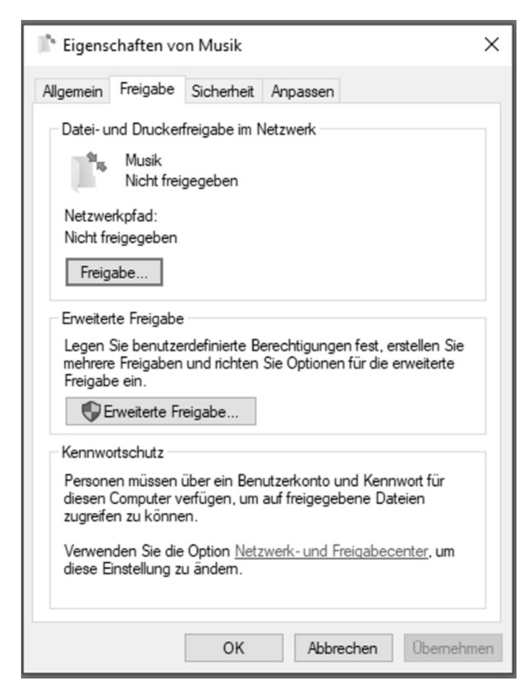


Abb. 19.28: Registerkarte FREIGABE des Ordners MUSIK

Klicken Sie auf ERWEITERTE FREIGABE, um das entsprechende Dialogfeld zu öffnen, und klicken Sie auf DIESEN ORDNER FREIGEBEN, um die Freigabe zu aktivieren (Abbildung 19.29). Hier können Sie eine Bezeichnung für die Freigabe vergeben. Standardmäßig wird der Name des Ordners übernommen, Sie können aber auch einen anderen verwenden. Zudem können Sie die Anzahl gleichzeitiger Benutzer beschränken und unter anderem einen Kommentar eingeben. Klicken Sie auf BERECHTIGUNGEN, um den letzten Schritt auszuführen (Abbildung 19.30).

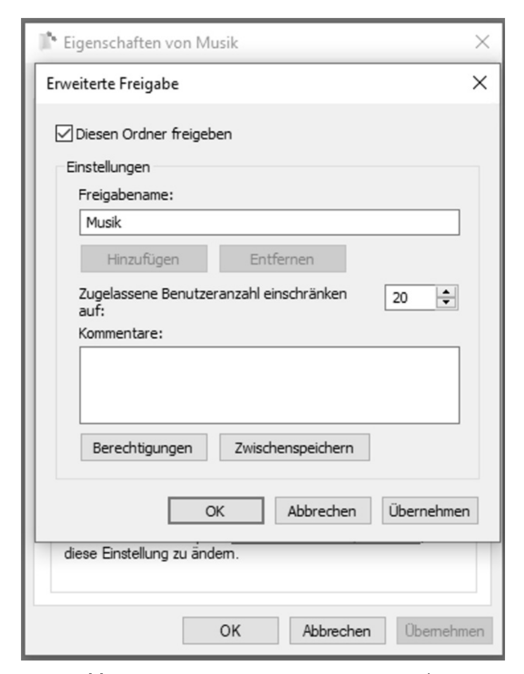


Abb. 19.29: Bereit zur erweiterten Freigabe

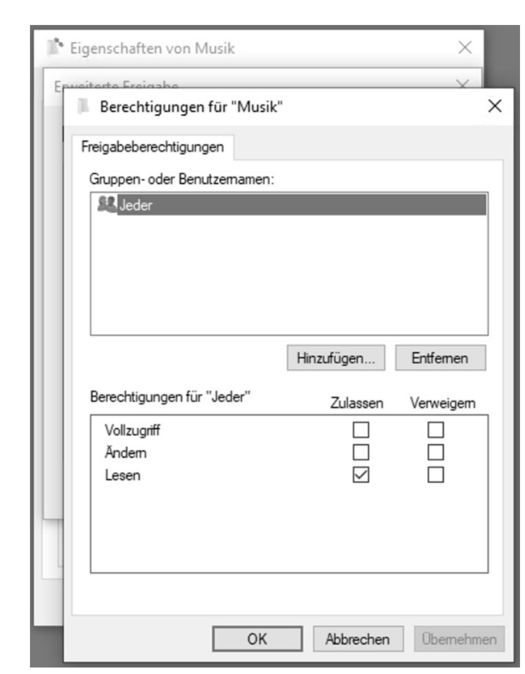


Abb. 19.30: Berechtigungen der erweiterten Freigabe

Für die Gruppe JEDER ist die Berechtigung LESEN voreingestellt, aber das lässt sich ändern. Sie können Benutzer und Gruppen hinzufügen oder entfernen. Klicken Sie auf HINZUFÜGEN, um das Dialogfeld BENUTZER ODER GRUPPEN AUSWÄHLEN zu öffnen, mit dem Sie nach Benutzern und Gruppen auf dem lokalen Rechner suchen können. (Das ist von Bedeutung, wie Sie im nächsten Punkt *Zugriff auf Ordnerfreigaben in Arbeitsgruppen* sehen werden.) Beachten Sie auch die übrigen Optionen.

Es gibt drei Berechtigungsebenen, nämlich Lesen, Schreiben und Vollzugriff, die Sie zulassen oder verweigern können. Wie bei den NTFS-Berechtigungen hat Verweigern stets Vorrang vor Zulassen. Die erweiterte Freigabe erlaubt es Ihnen, festzulegen, was bestimmte Benutzer und Gruppen mit einer Netzwerkfreigabe anstellen dürfen. Sie könnten beispielsweise allen Benutzern Vollzugriff gewähren, aber anschließend einem bestimmten Benutzer, vielleicht Robert aus der Buchhaltung, den Vollzugriff verweigern. In diesem Fall könnten alle Benutzer außer Robert auf die Ordnerfreigabe zugreifen, Dateien ändern, umbenennen, löschen und so weiter.

Wichtig

Rechnen Sie in der CompTIA A+-Prüfung 1002 mit Fragen, bei denen es um den Vergleich von NTFS- und Freigabeberechtigungen geht. NTFS bietet überlegene Steuerungsmöglichkeit für den Zugriff auf alle Ressourcen eines Computers. Freigabeberechtigungen beziehen sich lediglich auf Netzwerkfreigaben, wobei es keine Rolle spielt, ob sie mit dem Freigabe-Assistenten oder per erweiterter Freigabe erstellt wurden. Zulassen und Verweigern funktionieren in beiden Fällen auf die gleiche Art und Weise, wobei Verweigern stets Vorrang vor Zulassen hat.

Zugriff auf Ordnerfreigaben in Arbeitsgruppen Die Freigabe scheint offenbar recht ordentlich zu funktionieren, es gibt aber ein großes Problem: Beim Anmelden am Computer greifen Sie auf einen Benutzernamen und eine Datenbank zu. Die zugriffsberechtigten Benutzerkonten sind auf Ihrem Computer gespeichert. Wie können Sie nun dem Benutzer eines anderen Computers Zugriffsrechte auf einen freigegebenen Ordner gewähren? Sie müssen dieser Person einen gültigen Benutzernamen und ein dazugehöriges Kennwort zuweisen. Zur Nachverfolgung der Anmeldungen verwenden wir die Nomenklatur `<Computername\Benutzername>`. Wenn Sie sich am Computer A als Mike anmelden, sprechen wir davon, dass Sie als `ComputerA\Mike` angemeldet sind. Diese Notation ist äußerst praktisch, wenn vernetzte Computer Teil der betrachteten Vorgänge sind.

Abbildung 19.31 zeigt die beiden Computer A und B. Nehmen wir an, es gäbe einen freigegebenen Ordner namens STEFFI auf dem Computer A, für den Mike Schreib-/Leseberechtigungen besitzt.

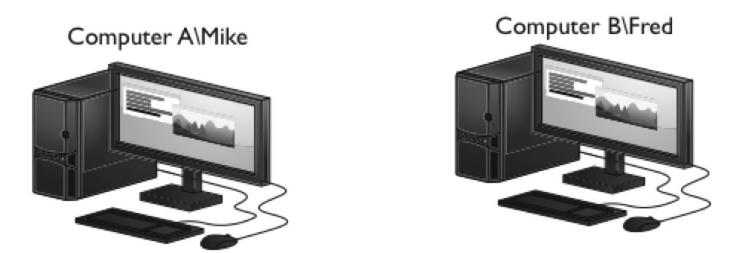


Abb. 19.31: Die Computer A und B

Nun schaltet jemand den Computer B ein und meldet sich als Fred an. Er lässt sich die Geräte im Netzwerk anzeigen und sieht den Computer A. Aber wenn er ihn anklickt, wird ihm ein Dialogfeld präsentiert, das zur Eingabe eines Netzwerkkennworts auffordert (Abbildung 19.32).

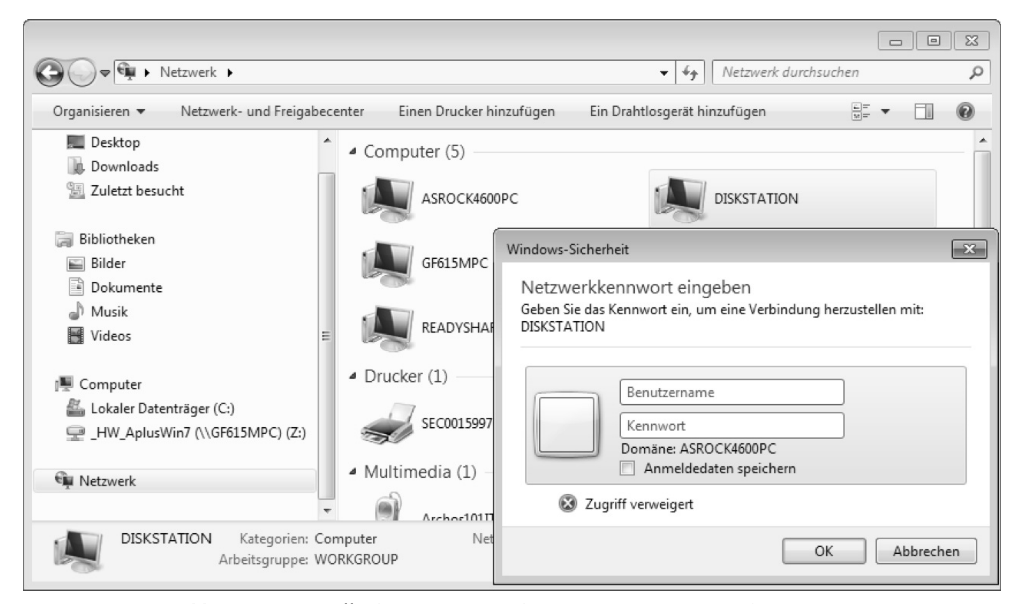


Abb. 19.32: Die Aufforderung zur Eingabe von Benutzername und Kennwort

Ursache hierfür ist, dass die Person als `ComputerB\Fred` angemeldet ist, sie aber als `ComputerA\Mike` angemeldet sein müsste, um auf den freigegebenen Ordner zuzugreifen. Der Benutzer muss also das

Kennwort für den `ComputerA\Mike` kennen. Nicht gerade die beste Methode, wenn es um die Sicherheit von Benutzernamen und Kennwörtern geht. Was also tun? Es gibt drei Möglichkeiten:

1. Sie sorgen dafür, dass sich die Leute wie eben beschrieben anmelden.
2. Sie legen auf allen Computern identische Benutzerkonten (derselbe Benutzername und dasselbe Kennwort) an und vergeben für alle Benutzer und Freigaben Zugriffsberechtigungen.
3. Sie verwenden auf allen Computern nur ein einziges Benutzerkonto. Alle Benutzer melden sich am selben Benutzerkonto an und alle Freigaben werden standardmäßig diesem Benutzerkonto zugewiesen.

Wichtig

Das Verschieben oder Kopieren von Dateien und Ordnern innerhalb einer Netzwerkfreigabe oder von einer Netzwerkfreigabe auf den lokalen Rechner hat keinen Einfluss auf die Dateiattribute. Wenn Sie beispielsweise eine schreibgeschützte Datei von einer Netzwerkfreigabe auf Ihren Desktop kopieren, ist sie noch immer schreibgeschützt. Sie können diese Dateiattribute aber leicht ändern, indem Sie mit der rechten Maustaste auf die Datei klicken und im Kontextmenü EIGENSCHAFTEN wählen.

Domänen

Arbeitsgruppen sind für kleinere Netzwerke (weniger als 30 Rechner) gut geeignet, aber in größeren Netzwerken, in denen mehr Kontrollmöglichkeiten erforderlich sind, ist es jedoch weitaus besser, eine Windows-*Domäne* zu verwenden, in der Benutzerkonten, Kennwörter und die Zugriffsberechtigungen auf Ressourcen zentral verwaltet werden. Sehen Sie sich Abbildung 19.33 und Abbildung 19.34 an. In einer Windows-Arbeitsgruppe verfügt jeder Computer über eigene lokale Benutzerkonten. In einer Windows-Domäne ist ein Computer, auf dem eine Windows-Serverversion läuft, als *Domänen-Controller* (*DC*) konfiguriert. Die Benutzerkonten des Domänen-Controllers heißen *Domänenkonten*. Die Benutzer können sich an jedem Computer in der Domäne mit demselben Domänenkonto anmelden.

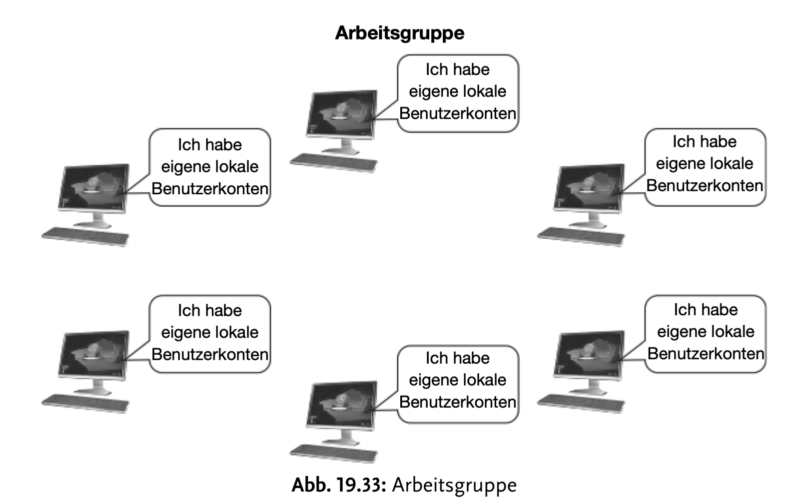


Abb. 19.33: Arbeitsgruppe

Hinweis

Auch wenn ein Computer zu einer Domäne gehört, können Sie sich mit einem lokalen Benutzerkonto anmelden, allerdings ist das nur selten erforderlich. Für gewöhnlich erfolgt das nur im Rahmen einer Fehlerbehebung, wie bei dem Wiederherstellen eines Benutzerprofils in Kapitel 16. Sobald Sie einer Domäne beigetreten sind, melden Sie sich ansonsten mit dem Domänenkonto an.

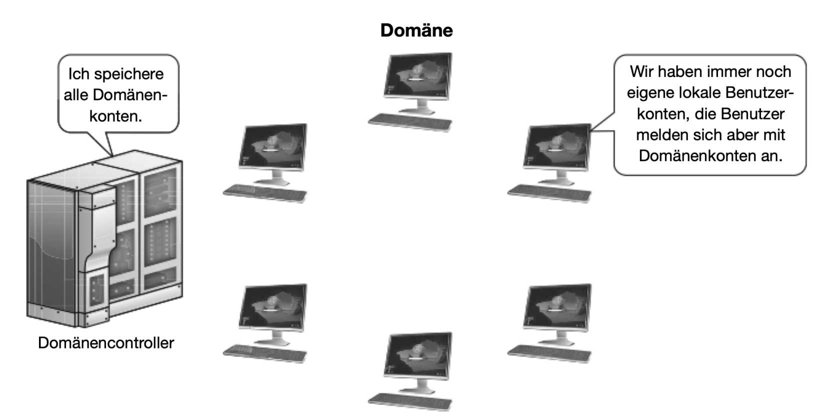


Abb. 19.34: Domäne

Eine Windows-Domäne ermöglicht es, sich an jedem Computer der Domäne mit demselben Domänenkonto anzumelden. Diese Funktion wird als *Einmalige Anmeldung* bezeichnet. Es ist nicht erforderlich, auf jedem Computer lokale Benutzerkonten anzulegen. Die Benutzerauthentifizierung durch ein einziges Domänenkonto gewährt Zugriff auf alle Rechner in der Domäne – daher auch die Bezeichnung »Einmalige Anmeldung«.

Wenn schon ein einzelner Computer sämtliche Benutzernamen und Kennwörter der Domäne speichert, warum dann nicht noch einen Schritt weitergehen und weitere Informationen über die Domäne speichern, wie etwa über vorhandene Drucker, Computernamen, Standortinformationen – alles, was irgendwie das gesamte Netzwerk betrifft? Moderne Windows-Versionen verwenden *Active Directory*, um genau diese Aufgaben zu erledigen. Zur Verwendung einer Domäne im Windows-Netzwerk benötigen Sie einen Computer, auf dem eine Server-Version von Windows läuft (Abbildung 19.35). Bei Windows Server handelt es sich um eine völlig unterschiedliche, erheblich leistungsfähigere und auch sehr viel teurere Version von Windows. Sie müssen diesen Server zu einem Domänen-Controller machen, wodurch ein Active Directory erstellt wird.

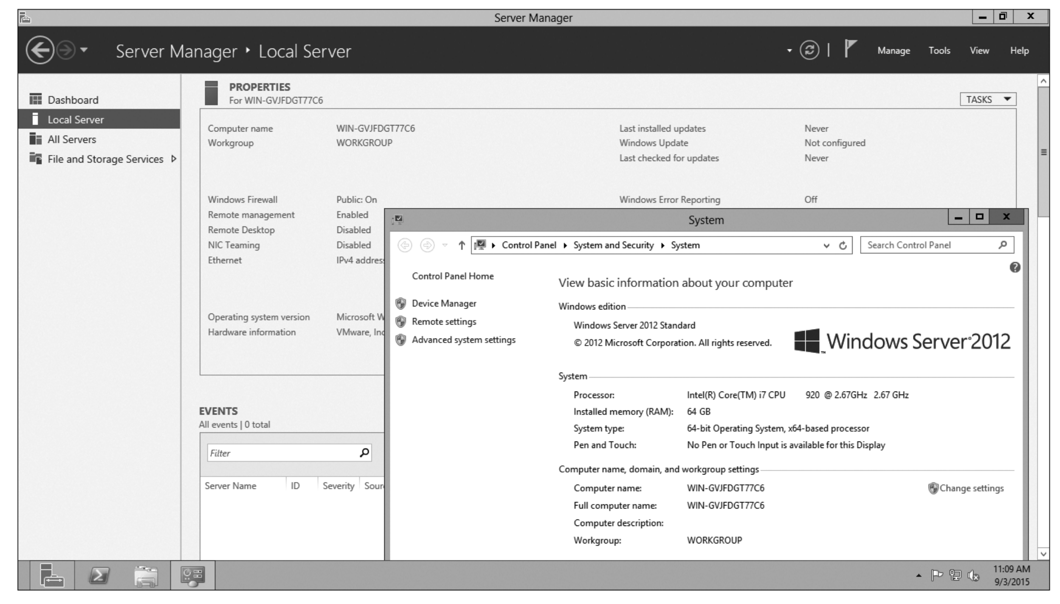


Abb. 19.35: Windows-Server

Sobald ein Rechner als Domänen-Controller eingerichtet ist und Active Directory verwendet, müssen alle PCs des Netzwerks dieser Domäne beitreten (dadurch werden die Rechner aus der Arbeitsgruppe entfernt). Wenn Sie sich nun an einem Computer anmelden, der Mitglied einer Domäne ist, fragt Windows Sie nach einem Benutzernamen, anstatt eine Liste mit Symbolen der Benutzer im Netzwerk anzuzeigen (Abbildung 19.36).

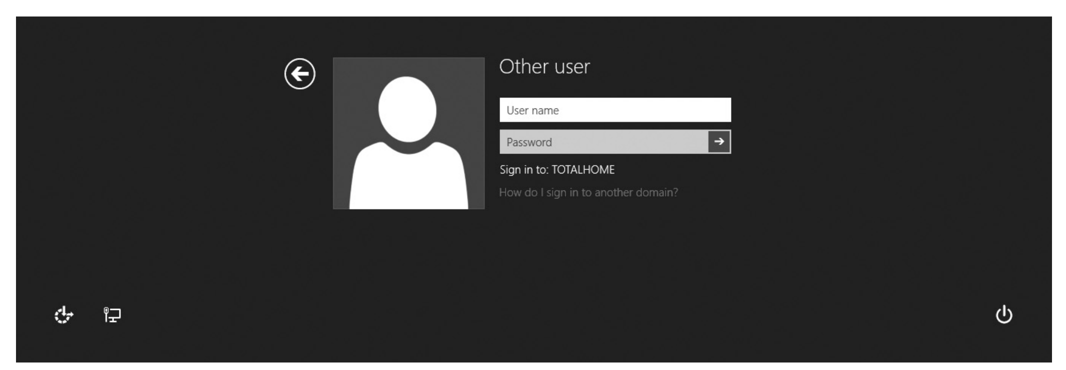


Abb. 19.36: Anmeldung an einer Domäne

Wenn Sie Active Directory verwenden, melden Sie sich nicht an Ihrem Computer an, sondern direkt beim Domänen-Controller. Alle Benutzerkonten sind auf dem Domänen-Controller gespeichert (Abbildung 19.37). Viele Domänen verwenden Bezeichnungen, die Ähnlichkeit mit Internetadressen haben, wie z.B. `totalhome.com` oder `totalhome.local`. Dank der vorhin erwähnten Nomenklatur können Sie sich mit `<Domänenname>\<Domänenbenutzername>` an einer Domäne anmelden. Wenn es beispielsweise in der Domäne `totalhome.local` ein Domänenbenutzerkonto namens `Mike` gäbe, würde man zur Anmeldung `totalhome.local\Mike` verwenden.

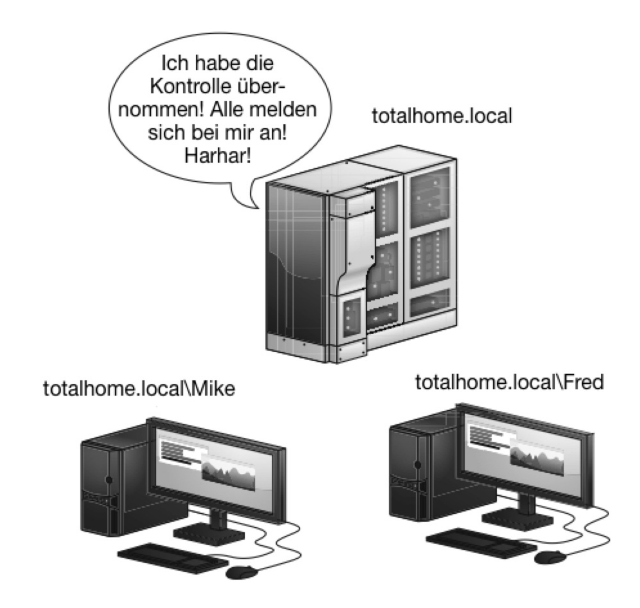


Abb. 19.37: Netzwerk mit Active Directory

Domänenorganisation Active Directory speichert alle Informationen über ein Netzwerk. Eine Möglichkeit, das Active Directory in Augenschein zu nehmen, ist die direkte Anmeldung an einem Domänen-Controller und die Ausführung von ACTIVE DIRECTORY-BENUTZER UND -COMPUTER – ein Werkzeug, das grundlegende Funktionen des Active Directory bereitstellt (Abbildung 19.38). Beachten Sie den Namen der Domäne auf der linken Seite (hier TOTALSEM.LOCAL). Die darunter befindlichen Ordner zeigen die Organisation der Domäne. Eigentlich handelt es sich nicht um Ordner, sondern um sogenannte Organisationseinheiten (sie sehen aber aus wie Ordner), aber mit der Definition warten wir noch einen Moment. Hier ist eine Liste der interessanteren Ordner:

- **Builtin**: An dieser Stelle sind die vordefinierten Domänengruppen gespeichert, wie etwa Domänenadministratoren und Benutzer.
- **Computers**: Hier sind alle Systeme der Domäne aufgeführt, vom Server bis zum Arbeitsplatzrechner.
- **Domain Controller**: Es kann nie schaden, mehr als einen Domänen-Controller zur Verfügung zu haben, falls mal einer ausfällt. Hier sind sie aufgelistet.
- **Users**: In diesem Bereich sind die nicht vordefinierten Benutzer der Domäne aufgeführt.

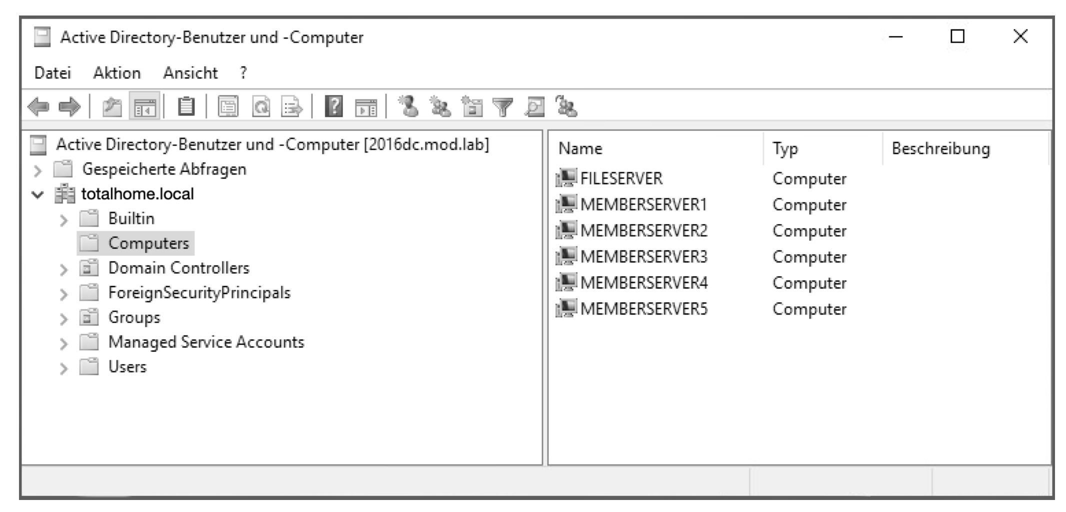


Abb. 19.38: Active Directory-Benutzer und -Computer

Domänenadministration Jedes einzelne System verfügt über ein Administratorkonto, und auch für die Domäne gibt es Domänenadministratoren. Diese Benutzerkonten sind außerordentlich mächtig und gestatten es, der Domäne weitere Computer hinzuzufügen. Für bestimmte Aufgaben sind die Berechtigungen eines Domänenadministrators erforderlich. Betrachten wir doch einmal, wie Computer und Benutzer zu einer Domäne hinzugefügt bzw. aus dieser entfernt werden.

Um einen Computer zu einer Domäne hinzuzufügen, wird das Dialogfeld verwendet, das auch beim Ändern des Namens einer Arbeitsgruppe zum Einsatz kam. Öffnen Sie in der Systemsteuerung das Applet SYSTEM, klicken Sie auf EINSTELLUNGEN ÄNDERN und auf der Registerkarte COMPUTERNAME auf NETZWERK-ID. Nun startet ein Assistent, der Sie zu dem Dialogfeld in Abbildung 19.39 führt. Vergewissern Sie sich, dass Sie über ein Domänenkonto verfügen, das der Domäne beitreten kann.

Um ein System aus einer Domäne zu entfernen, öffnen Sie ACTIVE DIRECTORY-BENUTZER UND -COMPUTER und klicken mit der rechten Maustaste auf den Computer, um an die Eigenschaften zu gelangen. Begeben Sie sich zur Registerkarte MITGLIED VON, wählen Sie den fraglichen Computer aus und klicken Sie auf ENTFERNEN (Abbildung 19.40).

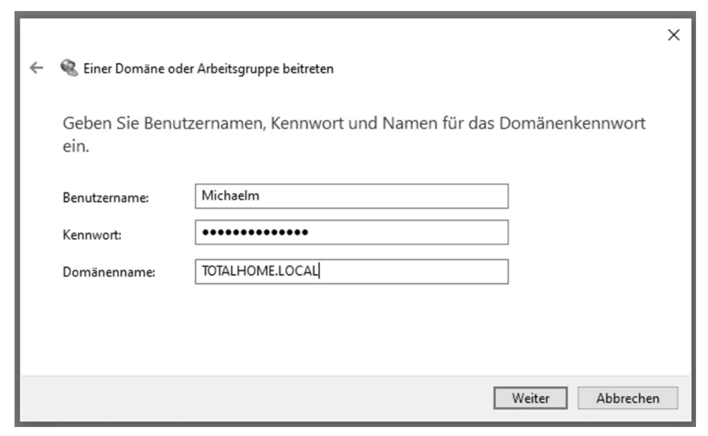


Abb. 19.39: Einer Domäne beitreten

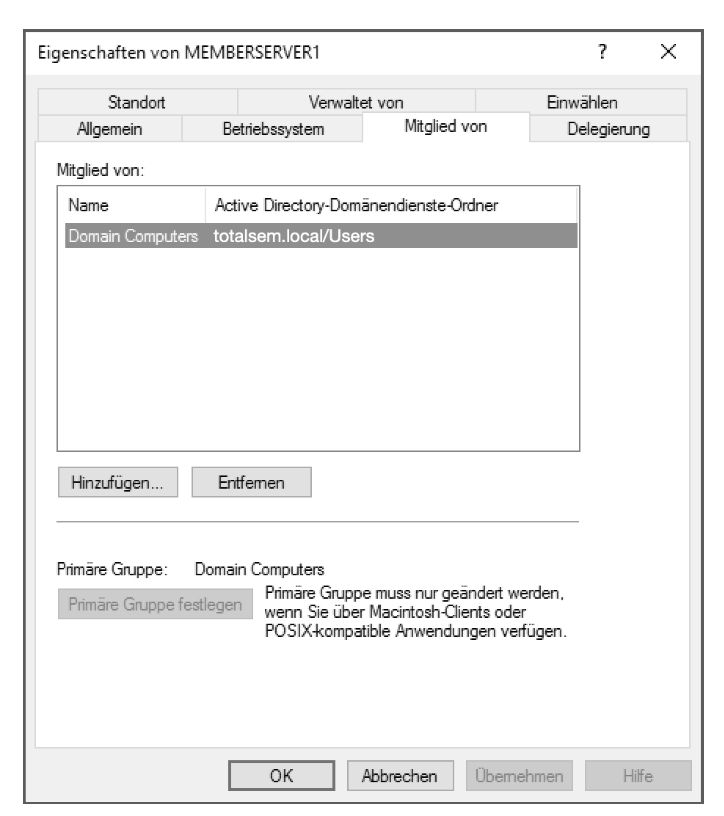


Abb. 19.40: Einen Computer aus einer Domäne entfernen

Es ist nicht möglich, aus einem lokalen Benutzer oder einer lokalen Benutzergruppe einen Domänenbenutzer bzw. eine Domänenbenutzergruppe zu machen. Der Domänenadministrator muss mit ACTIVE DIRECTORY-BENUTZER UND -COMPUTER ein neues Domänenkonto anlegen. Klicken Sie mit der rechten Maustaste auf USERS und wählen Sie NEU|BENUTZER aus (Abbildung 19.41), um das Dialogfeld NEUES OBJEKT – BENUTZER anzuzeigen. Abbildung 19.42 zeigt das ausgefüllte Dialogfeld.

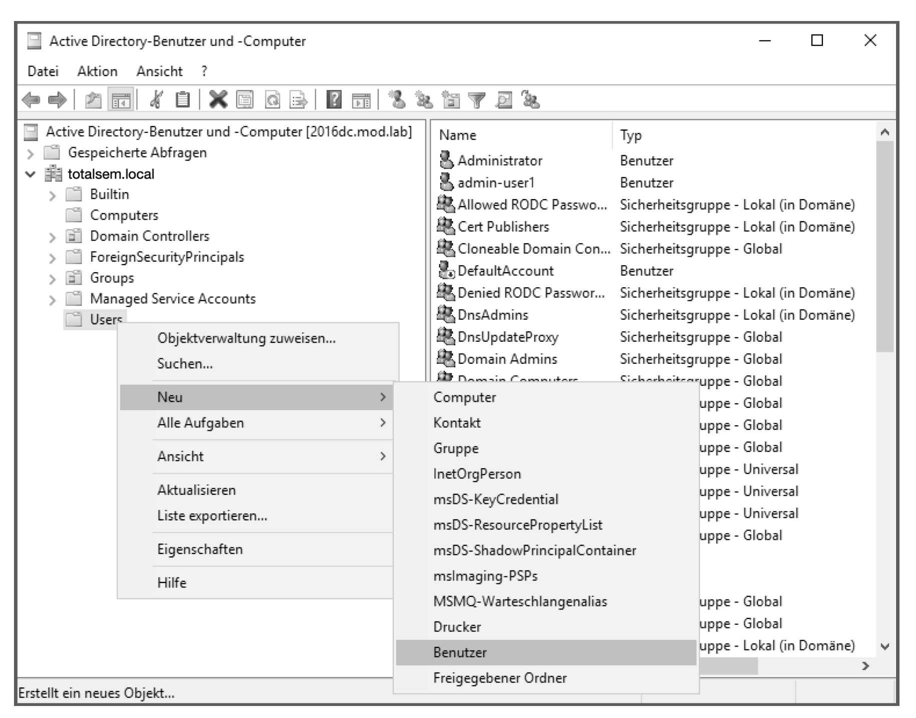


Abb. 19.41: Optionen des Kontextmenüs

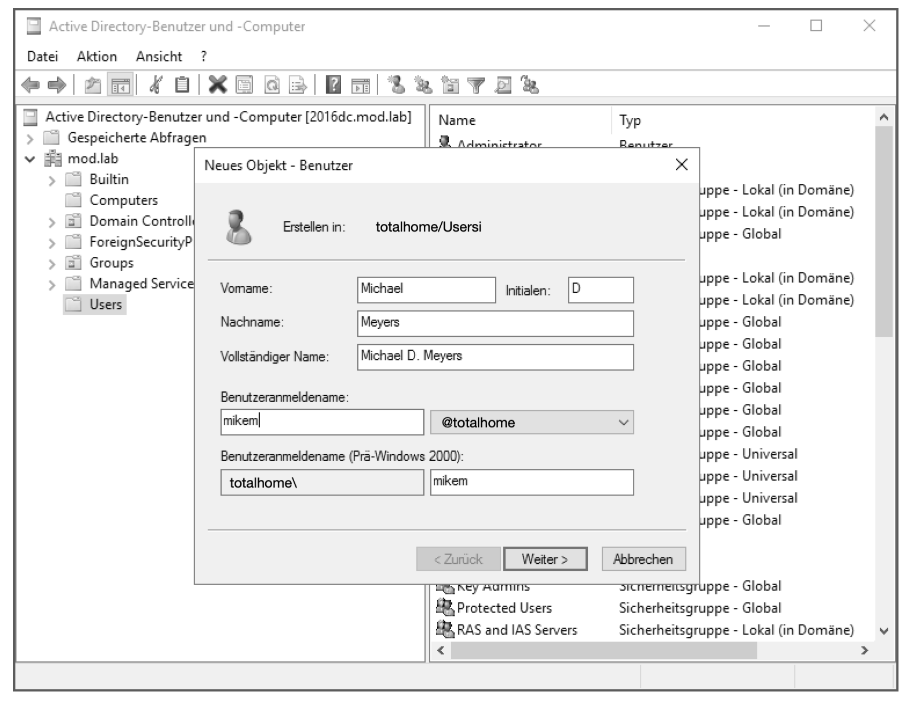


Abb. 19.42: Hinzufügen eines Domänenkontos

Der Domänenadministrator verwendet ACTIVE DIRECTORY-BENUTZER UND -COMPUTER auch, um Probleme mit Konten zu beheben. Um beispielsweise ein Kennwort zurückzusetzen, klicken Sie einen Benutzer mit der rechten Maustaste an und klicken auf KENNWORT ZURÜCKSETZEN, um das gleichnamige Dialogfeld zu öffnen (Abbildung 19.43). Geben Sie ein neues Kennwort ein, bestätigen Sie es und klicken Sie auf OK. In diesem Dialogfeld können Sie zudem das Kontrollkästchen SPERRE DES BENUTZERKONTOS AUFHEBEN markieren, falls sich jemand bei der Anmeldung wiederholt vertippt hat. Und schließlich können Sie ein Benutzerkonto im Kontextmenü durch Auswahl von BENUTZERKONTO AKTIVIEREN oder BENUTZERKONTO DEAKTIVIEREN – Sie haben es geahnt – aktivieren bzw. deaktivieren.

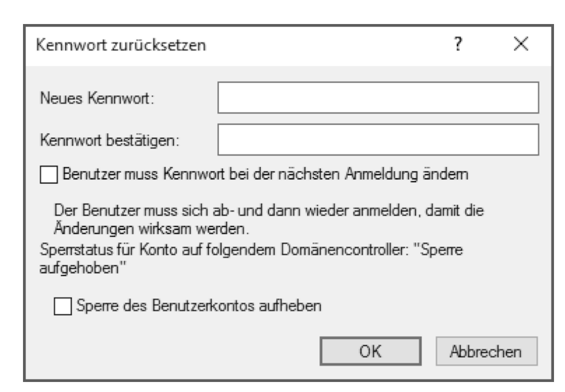


Abb. 19.43: Das Dialogfeld KENNWORT ZURÜCKSETZEN

Domänenkonten sind äußerst mächtig und bieten Features, die sich in lokalen Konten kaum finden. Sie können beispielsweise ein *Anmeldeskript* einrichten, das bei jeder Anmeldung des Benutzers ausgeführt wird. Damit können Sie Netzwerkfreigaben erstellen, Meldungen anzeigen, bestimmte Anwendungen ausführen (wie etwa Antimalware-Software) und viele andere Aufgaben erledigen. Sie müssen lediglich auf der Registerkarte PROFIL den Pfad und den Namen des Skripts angeben (Abbildung 19.44).

Abb. 19.44: Hinzufügen eines Anmeldeskripts

Active Directory bietet ein weiteres tolles Feature, nämlich die Möglichkeit, auszuwählen, wo das Home-Verzeichnis der Benutzer (Bilder, Downloads, Dokumente etc.) gespeichert wird. Dazu ist es erforderlich, statt eines lokalen Profils ein sogenanntes *Roamingprofil* zu verwenden. Das bedarf einer Erklärung. Bei jeder Anmeldung an einem Computer, den Sie noch nicht mit Ihrem Benutzerkonto verwendet haben, richtet Windows auf dem lokalen Rechner ein neues Home-Verzeichnis für Ihr Benutzerkonto ein. Es enthält jedoch nicht Ihre Daten, weil es neu angelegt wurde.

Das frustriert die Benutzer, weil sie jeweils nur einen Ordner für ihre Dokumente, Downloads, Bilder usw. verwenden wollen, also ein einziges, einheitliches Home-Verzeichnis. Um das zu erreichen, richten Administratoren Roamingprofile auf dem Server ein. Wenn der Benutzer sich an der Domäne anmeldet, tritt das Roamingprofil in Erscheinung und der Benutzer kann auf seine Dateien zugreifen.

Darüber hinaus können Administratoren den Speicherort des Home-Verzeichnisses festlegen, sodass angemeldete Benutzer auf ihr Home-Verzeichnis zugreifen können, das nicht auf dem lokalen Rechner, sondern auf einem entfernten Server gespeichert ist. Dieser Vorgang, der als *Ordnerumleitung* bezeichnet wird, ermöglicht Administratoren eine bessere Kontrolle über die Netzwerkressourcen.

Der Deutlichkeit halber: Die Einrichtung von Roamingprofilen und Ordnerumleitung (und anderer Features von Active Directory) nehmen Administratoren vor. Als CompTIA A+-Techniker müssen Sie jedoch wissen, dass es diese Features gibt.

Active Directory ermöglicht durch Organisationseinheiten eine äußerst flexible Organisation der Benutzer. Dabei handelt es sich um eine Art Behälter, der es gestattet, Benutzer und Computer anhand ihrer Aufgaben, ihres Standorts, ihrer Berechtigungen usw. zu organisieren. Was auch immer für Ihr Unternehmen sinnvoll erscheint, Sie können zur Verwaltung Organisationseinheiten verwenden.

Abbildung 19.45 zeigt das stark modifizierte Active Directory der Domäne `totalhome.local`. Beachten Sie, dass es Organisationseinheiten für verschiedene Standorte, inaktive Accounts und sogar Drucker gibt.

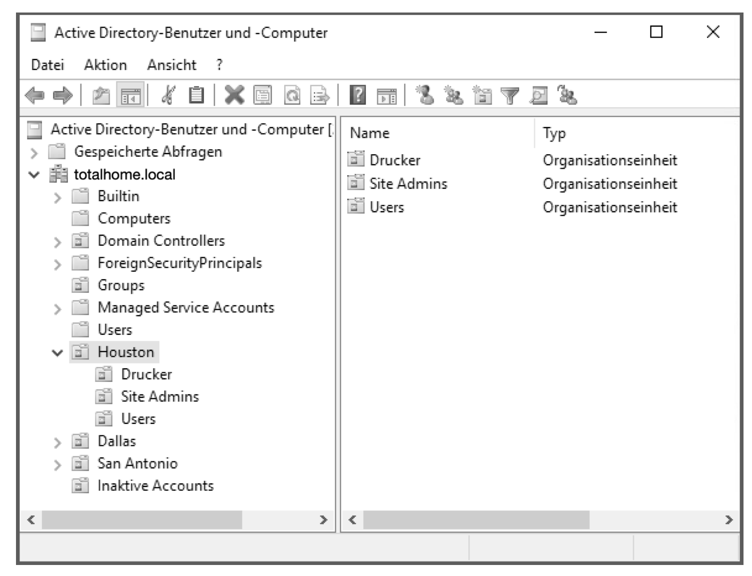


Abb. 19.45: Die Domäne `totalhome.local`

Wichtig

Der Domänen-Controller authentifiziert einen Benutzer, der sich an einem zur Domäne gehörigen Computer anmeldet. Der Domänen-Controller wird deshalb auch als Authentifizierungsserver bezeichnet.

Heimnetzgruppen

Das Problem bei der Verwendung von Arbeitsgruppen ist der fast komplette Mangel an Sicherheitsfunktionen und dass eine Unmenge von Anmeldungen erforderlich ist, um auf die Ressourcen zuzugreifen. Domänen hingegen erlauben einmaliges Anmelden und liefern vernünftige Sicherheitsfunktionen, erfordern jedoch dedizierte Server und eine ganze Menge Verwaltungsaufgaben. Um diesen Problemen zu begegnen, hat Microsoft mit Windows 7 eine Funktion namens *Heimnetzgruppe* eingeführt.

Hinweis

Heimnetzgruppen gibt es in Windows 7/8/8.1 und in den ersten Versionen von Windows 10. 2018 hat Microsoft die Unterstützung von Heimnetzgruppen in Windows 10 eingestellt. In der CompTIA A+-Zertifizierungsprüfung 1002 werden Heimnetzgruppen als ein Feature von Windows betrachtet. Das Lernziel 1.6 der CompTIA-Prüfung 1001 nennt den Vergleich Heimnetzgruppen und Arbeitsgruppen, also achten Sie auf Fangfragen.

Mit Heimnetzgruppen wird der Ansatz verfolgt, dass die Leute oft nicht daran interessiert sind, einen bestimmten Ordner freizugeben, sondern vielmehr gewisse Daten. Die meisten möchten beispielsweise ihre Musik oder ihre Bilder freigeben, nicht den Ordner MUSIK oder den Ordner BILDER. Konsequenterweise werden in Heimnetzgruppen daher Ordner übergangen und stattdessen die Bibliotheken von Windows freigegeben. Eine Heimnetzgruppe verbindet verschiedene Computer unter Verwendung eines gemeinsamen Kennworts; besondere Benutzernamen sind nicht erforderlich. Jeder Computer kann nur einer einzigen Heimnetzgruppe gleichzeitig angehören. Lassen Sie uns nun eine Heimnetzgruppe anlegen und feststellen, wie das Ganze funktioniert.

Wichtig

Heimnetzgruppen benötigen das IPv6-Protokoll, das glücklicherweise standardmäßig aktiviert ist.

Öffnen Sie in der Systemsteuerung das Applet HEIMNETZGRUPPEN, um eine neue Heimnetzgruppe anzulegen. Vorausgesetzt, Sie gehören einer Arbeitsgruppe an und haben noch keine Heimnetzgruppe angelegt, wird nun ein Dialogfeld wie in Abbildung 19.46 angezeigt.

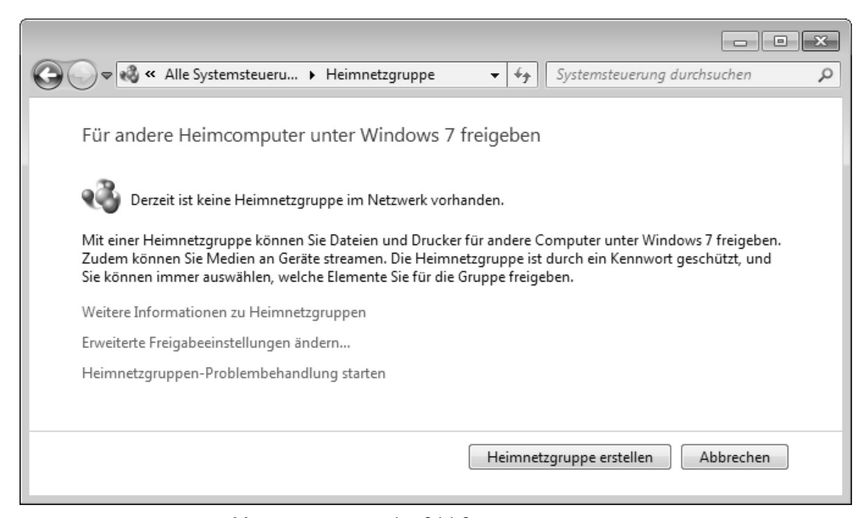


Abb. 19.46: Das Dialogfeld für Heimnetzgruppen

Klicken Sie auf die Schaltfläche HEIMNETZGRUPPE ERSTELLEN, um eine neue Heimnetzgruppe anzulegen. Es erscheint das Dialogfeld gleichen Namens (Abbildung 19.47).

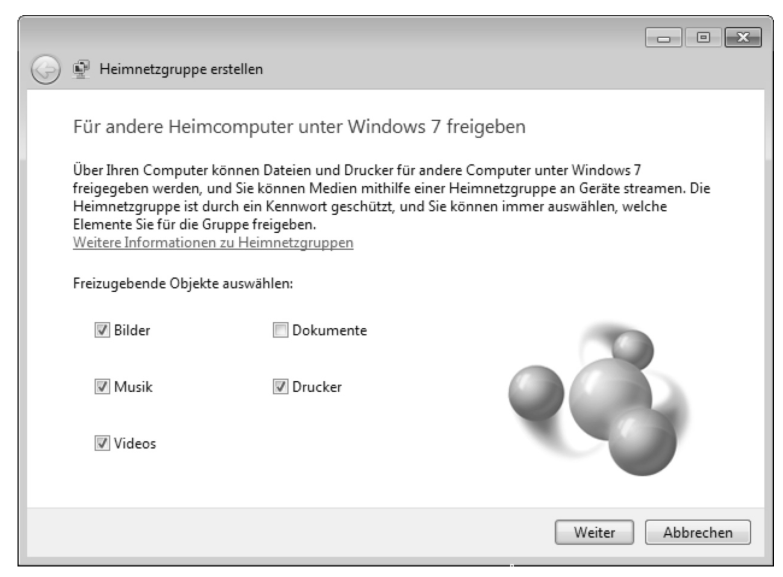


Abb. 19.47: Das Dialogfeld HEIMNETZGRUPPE ERSTELLEN

Beachten Sie die fünf Optionen: Bilder, Musik, Videos, Dokumente und Drucker. Das Ankreuzfeld für DOKUMENTE ist vermutlich nicht markiert, kreuzen Sie es also an, um alle fünf Objekte freizugeben. Klicken Sie auf WEITER, um das Kennwort der Heimnetzgruppe anzuzeigen (Abbildung 19.48).

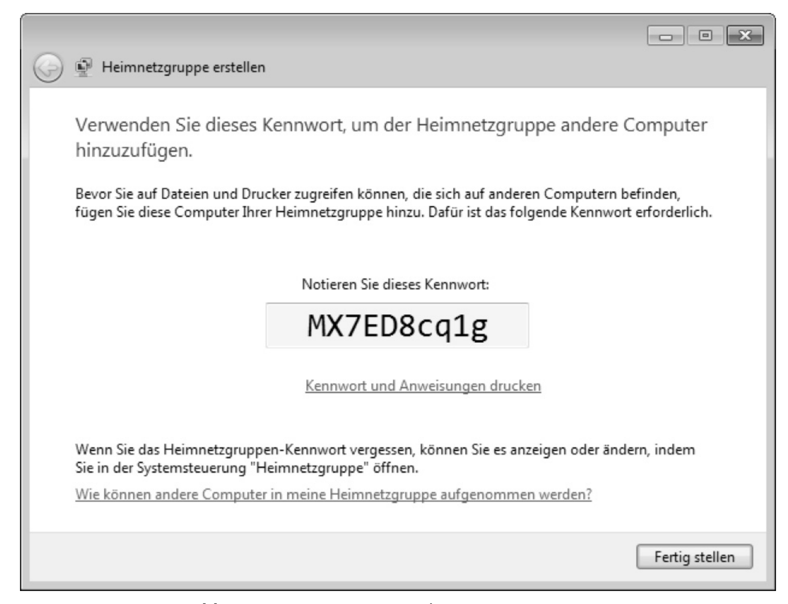


Abb. 19.48: Das Kennwort der Heimnetzgruppe

Hinweis

Bemerkenswerterweise findet die Datenübertragung zwischen den Systemen einer Heimnetzgruppe verschlüsselt statt.

Ihnen ist sicher schon zu Ohren gekommen, dass man Kennwörter nicht aufschreiben sollte? Tja, das angezeigte Kennwort ist so lang, dass Sie wohl kaum darum herumkommen. Das Dialogfeld bietet sogar eine Möglichkeit, das Kennwort auszudrucken. Klicken Sie erneut auf WEITER, um zu dem in Abbildung 19.49 gezeigten Dialogfeld zu gelangen. Dieses Dialogfeld wird künftig stets erscheinen, wenn Sie in der Systemsteuerung das Applet HEIMNETZGRUPPEN aufrufen.

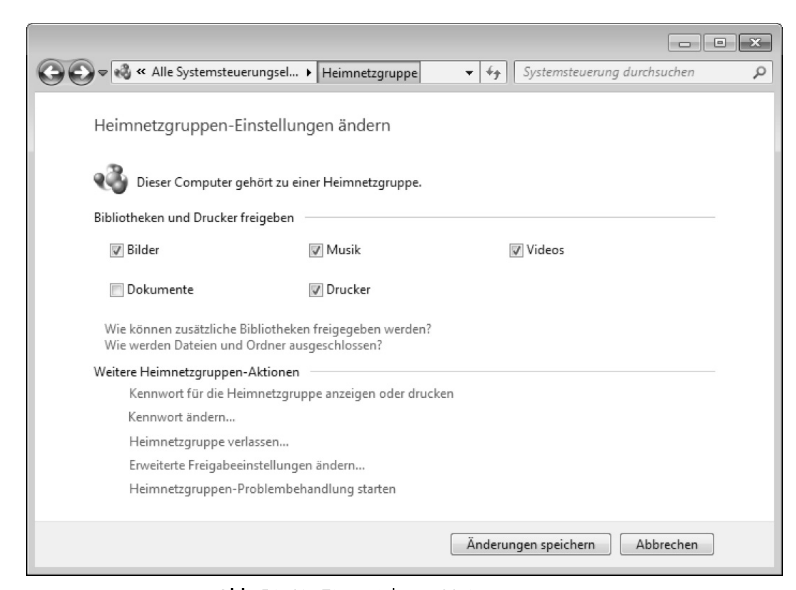


Abb. 19.49: Eingerichtete Heimnetzgruppe

Sehen Sie genau hin: Dort steht BIBLIOTHEKEN UND DRUCKER FREIGEBEN und etwas tiefer WIE KÖNNEN ZUSÄTZLICHE BIBLIOTHEKEN FREIGEGEBEN WERDEN?. Standardmäßig werden durch Heimnetzgruppen Bibliotheken freigegeben, nicht einzelne Ordner. Die Bibliotheken MUSIK, BILDER, VIDEOS und DOKUMENTE sind per Voreinstellung bereits freigegeben. Der Eintrag DRUCKER verfügt zwar über ein eigenes Ankreuzfeld, spiegelt jedoch die Einstellung der normalen Druckerfreigabe wider und ermöglicht es auch sporadischen Benutzern, schnell und einfach einen Drucker freizugeben.

Wichtig

Sie sollten sich merken, dass durch Heimnetzgruppen standardmäßig Bibliotheken freigeben werden, nicht Ordner.

Sobald Sie eine Heimnetzgruppe eingerichtet haben, können Sie diese an einem anderen Computer im Netzwerk überprüfen. Öffnen Sie dazu in der Systemsteuerung das Applet HEIMNETZGRUPPEN. Sofern die oben genannten Voraussetzungen erfüllt sind, sollte nun ein Dialogfeld wie in Abbildung 19.50 angezeigt werden.

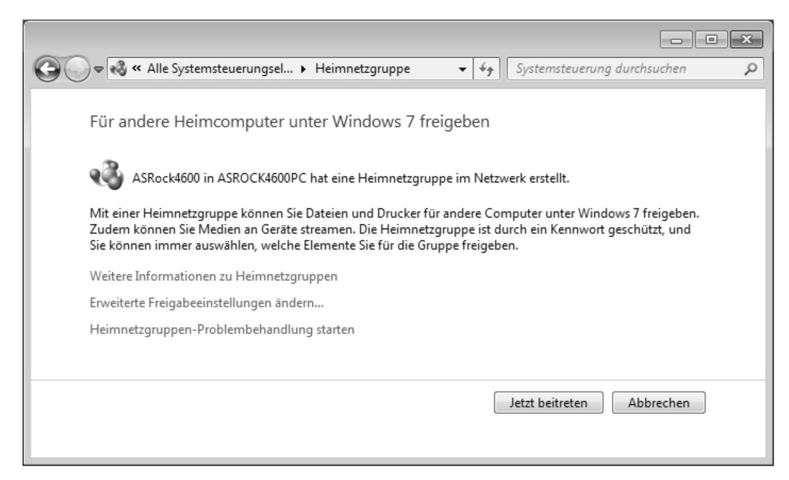


Abb. 19.50: Anzeige einer Heimnetzgruppe

Klicken Sie auf JETZT BEITRETEN, geben Sie das Kennwort ein und wählen Sie die Bibliotheken aus, die Sie für andere Benutzer freigeben möchten, und schon ist der neue Computer Teil der Heimnetzgruppe!

Sie können auf die per Heimnetzgruppe freigegebenen Dateien mit dem Windows-Explorer zugreifen (Abbildung 19.51). Wählen Sie den entsprechenden Computernamen aus, um sich anzeigen zu lassen, was andere Benutzer freigegeben haben. Anschließend können Sie diese Bibliotheken öffnen, um die freigegebenen Ordner in Augenschein zu nehmen.

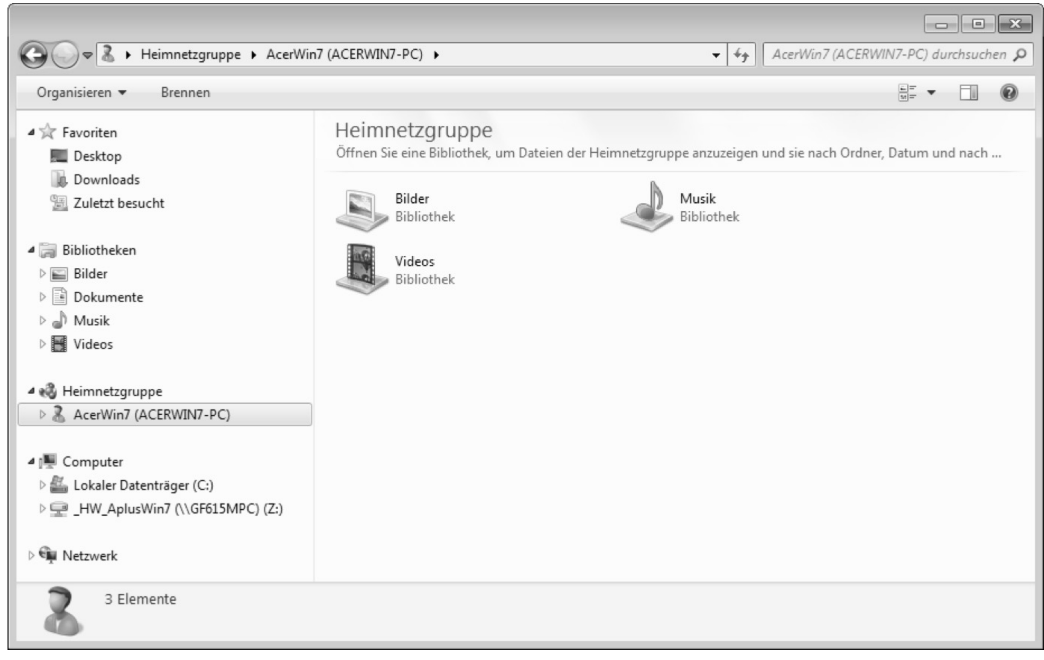


Abb. 19.51: Heimnetzgruppen verwenden

Hinweis

Nach dem Anlegen einer Heimnetzgruppe können Sie mit dem Windows-Explorer darauf zugreifen.

Weitere Bibliotheken freizugeben, ist ganz einfach, und falls Sie es wünschen, können Sie auch einzelne Ordner freigeben. Klicken Sie dazu mit der rechten Maustaste auf die Bibliothek oder den Ordner und wählen Sie wie in Abbildung 19.52 FREIGEBEN FÜR aus. Sie haben die Auswahl zwischen vier Optionen: NIEMAND, HEIMNETZGRUPPE (LESEN), HEIMNETZGRUPPE (LESEN/SCHREIBEN) und BESTIMMTE PERSONEN. NIEMAND bedeutet hier, dass das Objekt nicht freigegeben wird.

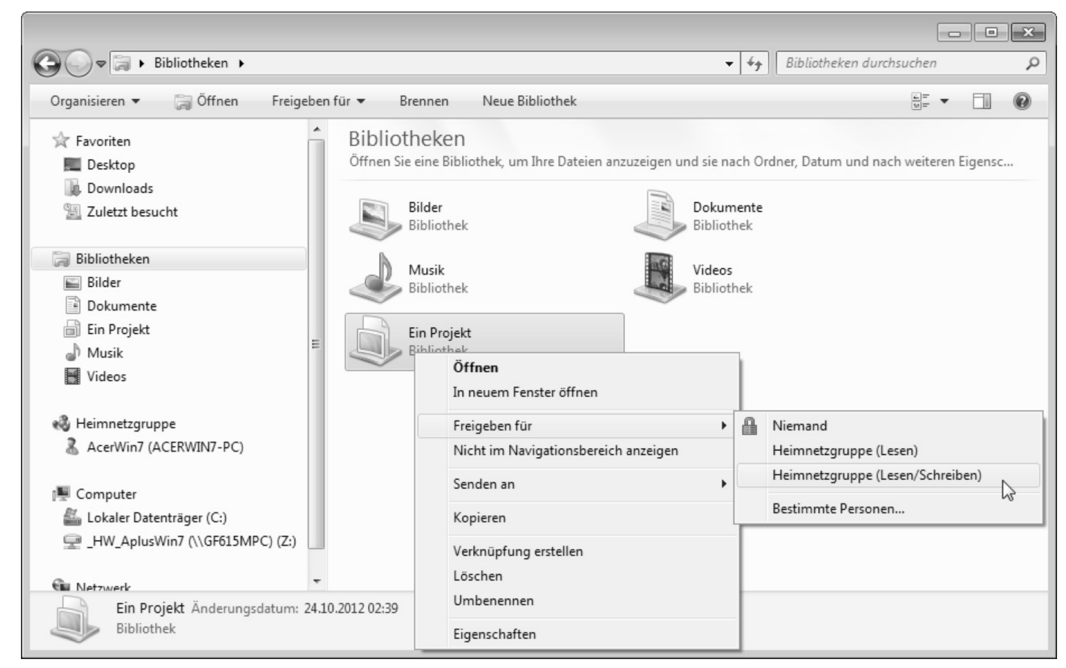


Abb. 19.52: Das Kontextmenü FREIGEBEN FÜR

Wichtig

Im Windows-Explorer wird eine Symbolleistenschaltfläche hinzugefügt, die genauso funktioniert wie das in Abbildung 19.52 gezeigte Menü.

Durch die Freigabe von Bibliotheken per Heimnetzgruppe verbirgt Microsoft die einzelnen Ordner vor den meisten Benutzern und erleichtert es den Anwendern, ihre Daten (Dokumente, Bilder, Musik und Videos) statt ihrer Ordner freizugeben. Heimnetzgruppen zielen auf eine ganz spezielle Umgebung ab: kleine Heimnetzwerke ohne Domäne, doch innerhalb dieses Rahmens funktionieren sie ausgezeichnet.

Druckerfreigabe

Die Freigabe von Druckern unter Windows ähnelt der Freigabe von Laufwerken und Ordnern. Wenn die Druckerfreigabe auf dem System aktiviert ist, wählen Sie in der Systemsteuerung das Applet GERÄTE UND DRUCKER aus und klicken dann mit der rechten Maustaste auf den Drucker, den Sie

freigeben möchten. Klicken Sie auf DRUCKEREIGENSCHAFTEN und wählen Sie die Registerkarte FREIGABE aus. Markieren Sie dort das Kontrollkästchen DRUCKER FREIGEBEN, vergeben Sie einen Namen und klicken Sie auf OK (Abbildung 19.53).

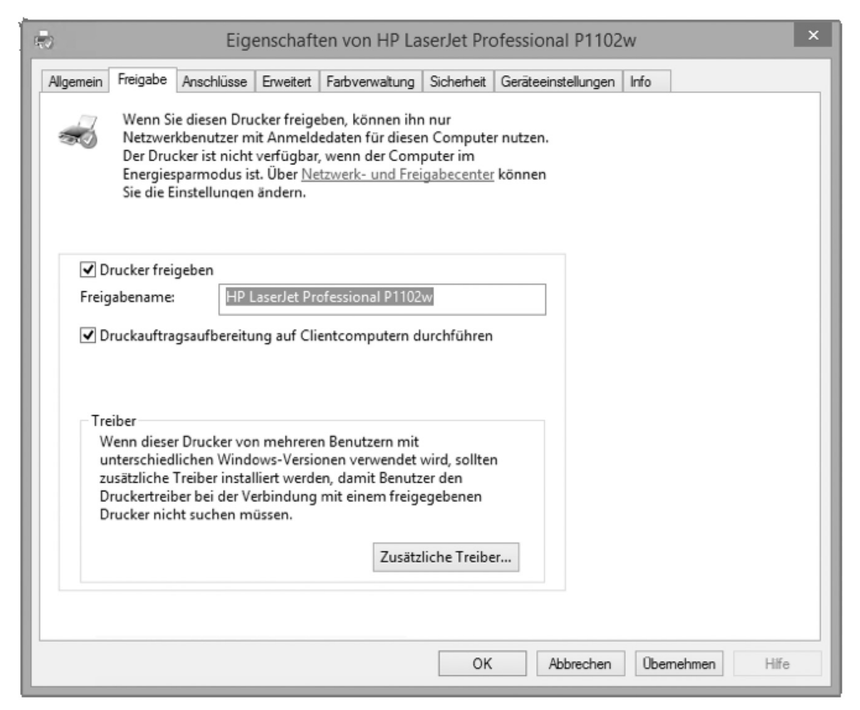


Abb. 19.53: Benennung eines freigegebenen Druckers

Hinweis

Wie der Zugriff auf freigegebene Drucker unter Windows funktioniert, erfahren Sie in Kapitel 26.

Einer der besten Aspekte an der Konfiguration eines Systems für die Verbindung mit einem Netzwerk ist die Tatsache, dass der Vorgang weitgehend automatisch abläuft. Wenn Windows z.B. eine Netzwerkkarte im System erkennt, dann installiert es automatisch einen Treiber für die Netzwerkkarte, ein Netzwerkprotokoll (TCP/IP) und den Client für Microsoft-Netzwerke. Wenn Sie eine Ressource freigeben wollen, dann wurden also alle erforderlichen Komponenten bereits installiert. Beachten Sie dabei aber, dass die Datei- und Druckerfreigabe zwar als Dienst automatisch installiert wird, dass Sie diesen aber anschließend, wie bereits erläutert, noch aktivieren müssen.

19.3 Problembehebung bei Netzwerken

Wenn Sie es nicht mehr mit einem einzelnen Rechner zu tun haben, sondern sich im Bereich vernetzter Rechner bewegen, dann müssen Ihre Fähigkeiten im Bereich der Problembehebung qualitativ einen gewaltigen Sprung vorwärtsmachen. Auf die Fragen der CompTIA im Zusammenhang mit Netzwerken die richtige Antwort zu finden, fällt leichter, wenn man sich daran erinnert, dass nur die Fähigkeit, einzelne Rechner wieder ins Netzwerk zu bekommen, geprüft wird. Fokussieren Sie sich darauf, einzelne Systeme wieder zum Laufen zu bekommen.

Hinweis

Die im Folgenden erläuterten Aspekte der Fehlerbehebung betreffen nur LANs und keine Probleme, die im Zusammenhang mit dem Internetzugang auftreten. Diese kommen in Kapitel 21 zur Sprache, sodass wir auf das in diesem Kapitel gewonnene Wissen aufbauen können.

Die CompTIA mag es offenbar, Fragen zu Themen wie »Kein Netzwerkzugriff« oder »Unterbrochener Netzwerkzugriff« zu stellen. Dabei sind zwei verschiedene Typen zu unterscheiden: Erstens gibt es Zugriffsprobleme, bei denen der Rechner physisch vom Netzwerk getrennt ist (darauf beziehen sich vermutlich die Fragen der CompTIA). Und zweitens gibt es Zugriffsprobleme, bei denen eine bestimmte Ressource nicht zugänglich ist, obwohl der Netzwerkzugriff an sich funktioniert. Wir werden beide Fälle betrachten.

Hinweis

Das Lernziel 5.1 der CompTIA A+-Prüfung bei der Fehlerbehebung bezieht sich auf eigenständige *und* vernetzte Computer. Sie kennen das bereits aus Kapitel 1. Denken Sie beim Lesen der nächsten Abschnitte über die Methoden zur Fehlerbehebung nach und wie sie auf Netzwerke anwendbar sind.

19.3.1 Reparaturen an der Verkabelung

»Das Netzwerk läuft nicht!« ist das Schlimmste, was ein Netzwerktechniker so zu hören bekommt. Es gibt zahlreiche Gründe für Netzwerkausfälle und eine professionell installierte Verkabelung von guter Qualität bereitet selten Probleme. Wenn aber doch, sollten Sie für diesen Fall gewappnet sein. Sehen wir uns mal an, was sich bei Schwierigkeiten mit dem physischen Netzwerk machen lässt.

Symptome

Der Verlust der physischen Netzwerkverbindung ist in Windows ziemlich offensichtlich. Windows zeigt ein rotes Kreuz im Infobereich an (Abbildung 19.54).



Abb. 19.54: Fehlersymbol im Infobereich

Wenn Ihnen dieses Problem begegnet, sollten Sie zunächst das Nächstliegende überprüfen. Starten Sie auf der Kommandozeile `ipconfig`. Besitzt das System eine APIPA/zeroconf-Adresse wie 169.254.15.22? Das ist ein deutlicher Hinweis darauf, dass die Verbindung zum DHCP-Server nicht funktioniert. Ist das Netzwerkkabel nicht im Rechner eingesteckt? Oder in der Wandsteckdose? Dann kontrollieren Sie die weniger offenkundigen Dinge: Ist die Netzwerkkarte im Geräte-Manager deaktiviert? Falls Sie hiermit nicht weiterkommen, werfen Sie einen Blick auf das andere Ende der Leitung. Wenn der Computer nicht mit einem funktionierenden Switch verbunden ist, gibt es ebenfalls entsprechende Fehlermeldungen.

Hinweis

Wenn Sie macOS oder Linux verwenden, können Sie mit den Befehlen `ifconfig` oder `ip` die gleichen Informationen wie mit dem Befehl `ipconfig` unter Windows anzeigen.

Nur temporär unterbrochene Verbindungen haben oft ähnliche Ursachen, die aber meist schwieriger aufzuspüren sind. Im nächsten Abschnitt können Sie herausfinden, wie Sie diesen ärgerlichen Verbindungsproblemen den Garaus machen.

Wichtig

Die Lernziele der CompTIA A+Prüfung 1001 nennt eine APIPA/zeroconf-Adresse als häufiges Symptom für Probleme mit dem drahtlosen oder kabelgebundenen Netzwerk, aber das ist nur die halbe Wahrheit. Eine APIPA- oder link-lokale Adresse statt einer richtigen Netzwerkadresse weist zweifelsohne auf eine fehlerhafte Verbindung mit dem DHCP-Server hin, die viele Ursachen haben kann. Aber heutzutage erhält jeder Computer eine link-lokale Adresse – so funktioniert IPv6 nun einmal.

In der Prüfung setzt die CompTIA jedenfalls link-lokale Adressen mit APIPA-Adressen gleich und könnte Sie womöglich in einer Frage durcheinanderbringen. Sie wissen es besser, aber beantworten Sie die Frage nicht falsch, nur weil Sie dem zu viel Bedeutung beimessen.

Untersuchen physischer Probleme

Halten Sie Ausschau nach Hinweisen auf eine physische Trennung der Netzwerkverbindung. Ein typisches Anzeichen dafür, dass ein physisches Problem bei der Netzwerkverbindung vorliegt, sind Fehlermeldungen wie »Server nicht gefunden« oder wenn bei Verwendung der zum Betriebssystem gehörenden Werkzeuge zum Durchsuchen des Netzwerks (wie etwa NETZWERK in Windows) nur das eigene System angezeigt wird.

Sollten mehrere Systeme gleichzeitig Probleme beim Zugriff auf das Netzwerk bekommen, deutet das oft auf Hardware-Probleme hin. Hier kommt Ihnen die Kenntnis der Netzwerkverkabelung zugute. Wenn plötzlich alle Systeme, die an einem bestimmten Switch hängen, nicht mehr aufs Netzwerk zugreifen können, andere Systeme jedoch tadellos arbeiten, haben Sie nicht nur ein Hardwareproblem, sondern auch einen Hauptverdächtigen, nämlich den fraglichen Switch.

Statusanzeige überprüfen

Falls Sie ein Hardwareproblem vermuten, überprüfen Sie als Erstes die Statusanzeigen der Netzwerkkarte und des Switches. Leuchten diese nicht, steht fest, dass die Verbindung irgendwo unterbrochen ist. Können Sie das betroffene Gerät nicht selbst in Augenschein nehmen (z.B. wenn Sie telefonisch Support leisten), bitten Sie den Anwender, das zu tun oder entsprechende Prüfsoftware zu verwenden.

Bleibt es dabei, dass das fragliche System keine Netzwerkverbindung aufbauen kann, sollten Sie ausschließen, dass ein defekter Switch oder andere größere Probleme dafür verantwortlich sind, indem Sie überprüfen, dass die anderen Benutzer auf Netzwerk und/oder Server zugreifen können. Untersuchen Sie auch das Verbindungskabel zwischen Wandsteckdose und PC. Falls die Möglichkeit besteht, schließen Sie das Kabel an einer bekanntermaßen funktionierenden Wandsteckdose an und testen Sie erneut, ob es funktioniert. Erfahrene Netzwerktechniker haben nur für diesen Zweck ein langes Patchkabel auf Lager. Sollte es damit tatsächlich wieder funktionieren, könnte das Verbindungskabel zwischen Switch und der Wandsteckdose für das Problem verantwortlich sein. Hat das Kabel vorher einwandfrei gearbeitet, sollten Sie die Stabilität von Verbindungen über dieses Kabel testen, z.B. durch einen längeren Testlauf mit `ping`.

Netzwerkkarte überprüfen

Achtung! Auch defekte Netzwerkkarten können die Ursache für ein nicht auffindbares Netzwerk sein. Verwenden Sie die Hilfsprogramme des Betriebssystems, um zu überprüfen, ob eine Netzwerkkarte ordnungsgemäß funktioniert. Falls es für die Netzwerkkarte spezielle Diagnose-Software gibt, sollten Sie diese auch nutzen, weil dabei die Funktionalität der Schaltkreise geprüft wird. Häufig ist die Buchse der Netzwerkkarte die Fehlerquelle, daher gibt es für viele Netzwerkkarten eine Software, um einen *Loopback-Test* durchzuführen. Dabei werden Daten an die Netzwerkkarte übertragen und geprüft, ob die Daten auch empfangen werden. Bei manchen Netzwerkkarten werden hier lediglich die Schaltkreise zum Senden und Empfangen getestet, nicht aber die physische Verbindung. Bei einem echten Loopback-Test kommt ein spezieller *Loopback-Stecker* zum Einsatz, der an die Netzwerkkarte angeschlossen wird Abbildung 19.55). Besteht die Netzwerkkarte diesen Test nicht, muss sie ersetzt werden.



Abb. 19.55: Loopback-Stecker

Hinweis

Die fest verbauten Netzwerkkarten in Laptops sind dafür berüchtigt, aufgrund des ständigen Ein- und Ausstöpselns kaputtzugehen. Bei einigen Laptops ist ein Austausch problemlos möglich, bei anderen ist ein neues Mainboard erforderlich. Oder verwenden Sie einen USB-Ethernet-Adapter.

Kabel überprüfen

Die weitaus meisten Probleme mit Netzwerkverbindungen treten im Bereich des Arbeitsplatzes auf. Wenn Sie dies ausschließen können, ist es an der Zeit, nach anderen, tieferliegenden Ursachen zu suchen.

Mit der richtigen Ausrüstung ist es nicht schwer, eine defekte Leitung der Horizontalverkabelung aufzuspüren. Wer ein Netzwerk betreibt, sollte sich auch ein entsprechendes Testgerät anschaffen, wie z.B. den Fluke MicroScanner, um damit die Impedanz der Leitung zu messen. Liefert die Messung eine nennenswerte Impedanz, dürfte das Kabel defekt sein. Mit etwas Erfahrung können Sie nicht nur feststellen, ob eine Verbindung unterbrochen ist, sondern auch, an welcher Stelle. Es ist zwar etwas Geduld erforderlich, insbesondere, wenn die Leitungen nicht ordentlich gekennzeichnet sind, aber Sie werden den Fehler schon finden.

Beim Leitungstest müssen Sie auch das Patchkabel berücksichtigen. Stecken Sie das Patchkabel vom PC ab, verbinden Sie es mit einem Loopback-Stecker und begeben Sie sich dann in den Telekommunikationsraum. Stecken Sie dort das entsprechende Patchkabel vom Switch ab und verbinden Sie es mit dem Testgerät, um einen vollständigen Leitungstest durchzuführen (Abbildung 19.56).

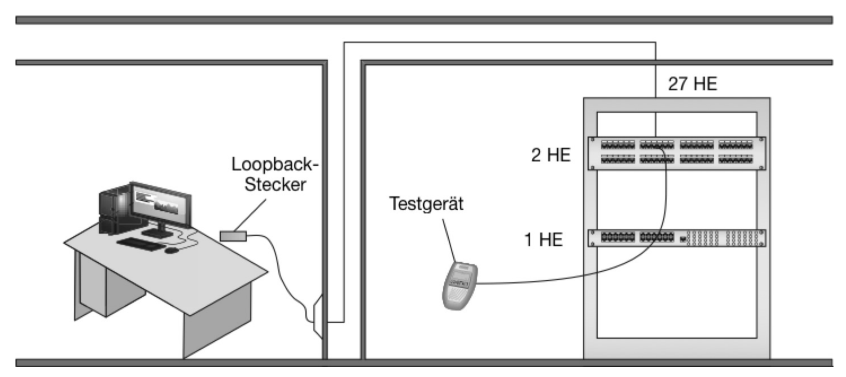


Abb. 19.56: Überprüfen einer Leitung

Auf diese Weise wird die gesamte Verbindung zwischen Switch und dem betroffenen System überprüft. Im Normalfall sind defekte Kabel zu ersetzen. Das ist bei einem Patchkabel leicht erledigt, aber was ist, wenn die Horizontalverkabelung defekt ist? In diesem Fall sollten Sie sich an Ihren Kabelinstallateur wenden. Wenn die Verkabelung an einer Stelle Fehler aufweist, ist das Risiko, dass es weitere Fehler gibt, zu hoch, als etwas anderes als eine vollständige Ersetzung auszuprobieren

Kabeltester

Es wäre schön, wenn man behaupten könnte, dass alle Verkabelungen perfekt funktionieren und nicht im Laufe der Jahre zu einem üblen, spaghettiartigen Haufen werden. Realistischerweise sollten Sie sich aber an den Gedanken gewöhnen, dass Sie früher oder später den Verlauf von Leitungen verfolgen müssen. Auch in hervorragend geplanten Netzwerken kommen Etiketten an Ports und Wandsteckdosen abhanden, tauchen mysteriöse Kabel hinter Verkleidungen auf, werden Leitungen hinzugefügt und Fehler beim Abzählen der Reihen und Spalten des Patchfeldes gemacht. Früher oder später passiert es jedenfalls fast jedem Netzwerktechniker, dass er ein Kabel nicht mehr zuordnen kann.

Beim Verfolgen des Leitungsverlaufs finden Kabeltester Verwendung. Dabei handelt es sich genau genommen um zwei Geräte: eines zum Erzeugen von Tönen und eine Tonsonde zum eigentlichen Testen (Abbildung 19.57). Der Tongenerator wird mit Krokodilklemmen oder Netzwerksteckern angeschlossen und sendet ein elektrisches Signal mit einer bestimmten Frequenz durch das Kabel. Die Tonsonde gibt Geräusche von sich, sobald sie sich in der Nähe eines Kabels befindet, das am Tongenerator angeschlossen ist. Diese beiden Geräte werden nach dem Markennamen eines verbreiteten Modells der Triplett Corporation auch *Fox and Hound* genannt.



Abb. 19.57: Tongenerator und Sonde

Schließen Sie den Tongenerator an einem Ende des fraglichen Kabels an und bringen Sie die Tonsonde in die Nähe der Kabel, die mögliche Kandidaten für das andere Ende sind. In der Nähe des richtigen Kabels beginnt die Tonsonde, zu piepsen. Es gibt auch Tonsonden, die mehrere Tongeneratoren erkennen, die Signale unterschiedlicher Frequenz aussenden und dadurch unterschieden wer-

den können. Selbst hochwertige Piepser sind relativ preiswert (ca. 70 Euro). Preisgünstigere Geräte um die 20 Euro arbeiten oft nicht zuverlässig, sparen Sie daher hier nicht am falschen Ende. Wenn Sie ein Netzwerk betreuen, sollte auch ein ordentlicher Piepser zu Ihrer Ausrüstung gehören.

19.3.2 Behebung typischer Probleme

Kommen wir zurück zu den Zugriffsproblemen, bei denen eine Ressource nicht zugänglich ist, obwohl der eigentliche Netzwerkzugriff funktioniert. Es kommt ziemlich häufig vor, dass die Verbindung zu einer freigegebenen Ressource nicht hergestellt werden kann oder dass eine vormals verwendete Ressource plötzlich nicht mehr zur Verfügung steht. Das bezieht sich (zumindest in diesem Kapitel) auf lokale Ressourcen – Netzwerkfreigaben, Druckerfreigaben, E-Mail-Server und so weiter. Zugriffsprobleme auf nicht zugängliche Ressourcen zu beheben, gehört für Techniker zum Alltag.

Die Verbindung zu einer neu freigegebenen Ressource funktioniert nicht

Wenn die Verbindung zu einer neu freigegebenen Ressource nicht auf Anhieb funktioniert, ist das oft ein Hinweis auf Konfigurationsfehler. Häufig zeigt eine erneute Überprüfung eines der folgenden Probleme (und einen Weg zur Lösung):

- Ist die Bezeichnung der Freigabe korrekt? Überprüfen Sie den Namen.
- Fehlt Ihnen der erforderliche Benutzername bzw. das Kennwort? Erkundigen Sie sich danach oder überprüfen Sie, ob Ihr Benutzerkonto die notwendigen Zugriffsberechtigungen besitzt.
- Ihnen fehlen die Zugriffsrechte, um die freigegebene Ressource zu nutzen? Holen Sie sich die Zugriffsrechte.
- Ihr Rechner ist nicht Mitglied der richtigen Heimnetzgruppe, Domäne oder Arbeitsgruppe? Prüfen Sie, welchen Domänen- oder Arbeitsgruppennamen Sie verwenden müssen. In einer Heimnetzgruppe sollten Sie sich vergewissern, dass Sie das korrekte Kennwort verwenden.
- Der Ordner oder Drucker ist gar nicht freigegeben? Geben Sie ihn frei!
- Der Ordner oder Drucker ist nicht vorhanden? Stellen Sie sicher, dass der Server den Ordner, auf den Sie zugreifen möchten, tatsächlich bereitstellt. Richten Sie den Drucker für den Netzwerkzugang ein, falls Sie das noch nicht erledigt haben.

Die Verbindung zu einer bereits genutzten Ressource funktioniert nicht mehr

Wenn Sie plötzlich nicht mehr auf eine Ressource zugreifen können, die Sie vorher schon oft benutzt haben, überprüfen Sie zunächst folgende Punkte:

- Prüfen Sie mittels NETZWERK, ob Ihnen die Ressource angezeigt wird.
- Vergewissern Sie sich, dass der Server überhaupt eingeschaltet ist.
- Überprüfen Sie auch, ob Ihr System physisch mit dem Server verbunden ist.

Der Befehl net

Unter Windows können Sie sich mit dem Befehl `net` schnell über ein Netzwerk informieren. Das ist dann besonders sinnvoll, wenn Sie einen Rechner erstmals mit einem Netzwerk verbinden und die Namen der anderen Rechner im Netzwerk nicht kennen. Um sich die vielen Optionen des `net`-Befehls anzeigen zu lassen, geben Sie an der Eingabeaufforderung `net` ein und betätigen ↵. Bei den Optionen `view` und `use` handelt es sich um hervorragende Netzwerkhelferlein.

Sie können sich `net view` als die Befehlszeilenversion der Netzwerkumgebung vorstellen. Wird `net view` ausgeführt, dann wird eine Liste der Windows-Rechner im Netzwerk ausgegeben:

```
C:\>net view
Servername            Kommentar
----------------------------------------------------
```

```
\\SABERTOOTH
\\UBERBOX
\\SERVER1
Der Befehl wurde erfolgreich ausgeführt.
```

Wenn Sie die Namen der Rechner erst einmal kennen, dann können Sie `net view` gefolgt vom Computernamen eingeben. `net view` zeigt dann alle Freigaben auf dem Rechner an und teilt Ihnen mit, ob es sich dabei um verbundene Laufwerke handelt.

```
C:\>net view server1
Freigegebene Ressourcen auf SERVER1
Freigabename   Typ      Verwendet als   Kommentar
-------------------------------------------------
FREDC          Platte
Forschung      Platte   W:
Der Befehl wurde erfolgreich ausgeführt.
```

Bei `net use` handelt es sich um die Befehlszeilenversion zum Verbinden mit Netzwerkfreigaben. Wenn Sie z.B. die Freigabe FORSCHUNG aus dem letzten Beispiel mit dem Laufwerk X: verbinden wollen, dann geben Sie einfach dies ein:

```
C:\>net use x: \\server1\Forschung
```

Damit wird die Freigabe FORSCHUNG auf dem Computer `SERVER1` mit dem Laufwerk X: auf dem lokalen Rechner verbunden.

Hinweis

Der Befehl `net` verschafft Ihnen einen schnellen Überblick über die Einstellungen des Windows-Netzwerks, etwa Computername, Betriebssystemversion, Name der Domäne oder Arbeitsgruppe und anderes mehr. Geben Sie `net config workstation` ein. Schnell und einfach!

Der Befehl nbtstat

Dieser Befehl ist ein altes Hilfsprogramm, das noch aus Zeiten vor Windows stammt. Er kürzt *NetBIOS over TCP/IP Statistics* ab. Sehr alte Windows-Versionen nutzten NetBIOS für verschiedene Aspekte von Freigaben. Auch wenn NetBIOS längst nicht mehr verwendet wird, kann man sich beispielsweise die Hostnamen eines Netzwerks anzeigen lassen, wenn kein DNS-Server verfügbar ist.

Der Befehl ist zwar nicht mehr so nützlich wie damals, mit `nbstat` kann man aber immer noch Probleme mit Rechnernamen in kleinen Arbeitsgruppen erforschen. Es folgen einige Beispiele für die Anwendung dieses Befehls. Geben Sie `nbstat -n` ein, um den NetBIOS-Namen Ihres Rechners anzuzeigen:

```
C:\>nbtstat -n
Local Area Connection:
Node IpAddress: [192.168.4.43] Scope Id: []
           NetBIOS Local Name Table
  Name            Type            Status
---------------------------------------------
mmyers-ws    <00> UNIQUE        Registered
WORKGROUP    <00> GROUP         Registered
mmyers-ws    <20> UNIQUE        Registered
```

Sie können sich die einem Rechner bekannten NetBIOS-Namen anzeigen lassen, wenn Sie dessen IP-Adresse kennen. Beachten Sie den Großbuchstaben »A«. Verwenden Sie ein kleines »a«, wenn Sie den NetBIOS-Namen bereits kennen.

```
C:\>nbtstat -A 192.168.4.43
Local Area Connection:
Node IpAddress: [192.168.4.43] Scope Id: []
      NetBIOS Remote Machine Name Table
  Name              Type          Status
--------------------------------------------
UNITEDKINGDOM  <00> UNIQUE      Registered
UNITEDKINGDOM  <03> UNIQUE      Registered
UNITEDKINGDOM  <20> UNIQUE      Registered
..__MSBROWSE__.<01> GROUP       Registered
TOTALHOME      <00> GROUP       Registered
TOTALHOME      <1D> UNIQUE      Registered
TOTALHOME      <1E> GROUP       Registered

MAC Address = 00-00-00-00-00-00
```

Und so zeigen Sie alle im lokalen Cache befindlichen Rechnernamen an, die NetBIOS kennt:

```
C:\>nbtstat -c
Local Area Connection:
Node IpAddress: [192.168.4.43] Scope Id: []
      NetBIOS Remote Cache Name Table
  Name              Type    Host Address   Life [sec]
-----------------------------------------------------
CLASS-SERVER   <00> UNIQUE  192.168.4.50      447
CLASS-SERVER   <20> UNIQUE  192.168.4.50      447
TOTALHOME      <1B> UNIQUE  192.168.4.12      450
UNITEDKINGDOM  <20> UNIQUE  192.168.4.52      417
UNITEDKINGDOM  <00> UNIQUE  192.168.4.52      417
WIN7-64        <20> UNIQUE  192.168.4.220     450
```

Da der Cache nur temporär vorhanden ist, werden Sie womöglich feststellen, dass er leer ist, wenn Sie zuvor nicht auf andere Rechner im LAN zugegriffen haben.

19.4 Wiederholung

19.4.1 Fragen

1. Das Windows-System von Stefan kann sich nicht mehr mit dem Internet verbinden und er bittet Sie um Hilfe. Sie vermuten, dass es sich um ein DHCP-Problem handelt. Welchen Befehl bzw. welches Programm sollten Sie ausführen, um den Fehler clientseitig zu finden und zu beheben?
   A. `ipconfig`
   B. `ifconfig`
   C. `config`
   D. `dhcp /renew`

2. Welchen Befehl würden Sie verwenden, um den Weg anzuzeigen, den ein Ethernet-Paket nimmt?
   A. `ping`
   B. `ipconfig`
   C. `tracert`
   D. `nslookup`
3. Wie lautet die korrekte Syntax, um herauszufinden, welche Netzwerkfreigaben eines bestimmten Dateiservers auf Ihrem Computer abgebildet sind?
   A. `net view \\DATEISERVER`
   B. `net \\DATEISERVER`
   C. `net map \\DATEISERVER`
   D. `net share \\DATEISERVER`
4. Welches kleine Gerät ermöglicht es Ihnen, die Schaltkreise einer Netzwerkkarte zu überprüfen?
   A. Loopback-Stecker
   B. Port-Tester
   C. Multimeter
   D. Integrierte Netzwerk- und Logiksonde
5. Welcher Befehl kann verwendet werden, um die gecachten NetBIOS-Namen eines Windows-Systems anzuzeigen?
   A. `nslookup`
   B. `dig --cache`
   C. `nbtstat -c`
   D. `nbtstat -a`
6. Sie kriechen gerade unter Ihrem Schreibtisch umher und ordnen einige Kabel, als Sie bemerken, dass die Aktivitätsanzeige der Netzwerkkarte unregelmäßig blinkt. Gibt es ein Problem?
   A. Ja, die Aktivitätsanzeige sollte bei eingeschaltetem Computer konstant leuchten.
   B. Ja, die Aktivitätsanzeige sollte regelmäßig blinken, nicht unregelmäßig.
   C. Nein, die Anzeige blinkt, wenn Datenverkehr stattfindet.
   D. Nein, die Anzeige blinkt, um auf Busaktivität hinzuweisen.
7. Was ist ein typischer Hinweis auf ein defektes Netzwerkkabel?
   A. Unregelmäßig blinkende Verbindungsstatusanzeige
   B. Verbindungsstatusanzeige leuchtet nicht.
   C. Konstant leuchtende Verbindungsstatusanzeige
   D. Regelmäßig blinkende Verbindungsstatusanzeige
8. Welchen Befehl würden Sie verwenden, um eine Liste der Computer im Netzwerk anzuzeigen?
   A. `net send`
   B. `show net_servers`
   C. `net use`
   D. `net view`
9. Welchen Vorteil hat der Vollduplex-Modus?
   A. Er erlaubt Netzwerkkarten das gleichzeitige Senden und Empfangen von Daten.
   B. Er erlaubt es Netzwerkkarten, Daten doppelt so schnell zu versenden.
   C. Er erlaubt es Netzwerkkarten, Daten doppelt so schnell zu empfangen.
   D. Er ermöglicht es, am Switch sowohl Koaxial- als auch Glasfaserkabel anzuschließen.

10. Wie nennen viele Techniker einen Kabeltester?
    A. ISDN
    B. UTP
    C. UDP
    D. Fox and Hound

19.4.2 Antworten

1. **A.** Sie sollten `ipconfig` ausführen, um Stefans Windows-System über DHCP eine neue IP-Adresse zuweisen zu lassen, genauer `ipconfig /release` und `ipconfig /renew`. Normalerweise lassen sich clientseitige DHCP-Probleme dadurch beheben. In Linux und macOS heißt das Programm, das dazu verwendet wird `ifconfig`. `config` und `dhcp` sind keine gültigen Befehle.
2. **C.** Der Befehl `tracert` verfolgt den Weg eines Datenpakets bis an dessen Bestimmungsort. In macOS und Linux heißt der Befehl `traceroute`.
3. **A.** Um die abgebildeten Netzwerkfreigaben anzuzeigen, wird das Kommando `net view \\DATEI-SERVER` verwendet.
4. **A.** Mit einem Loopback-Stecker können Sie die Schaltkreise einer Netzwerkkarte prüfen.
5. **C.** `nslookup` und `dig` funktionieren nur mit einem DNS-Server, nicht mit NetBIOS. `nbtstat -a` zeigt die Namen entfernter Systeme an, `nbtstat -c` zeigt die gecachten Namen an.
6. **C.** Die Anzeige blinkt, um Aktivität anzuzeigen – das ist völlig normal.
7. **B.** Wenn die Verbindungsstatusanzeige nicht leuchtet, handelt es sich vermutlich um ein defektes Kabel.
8. **D.** Der Befehl `net view` zeigt eine Liste der Computer im Netzwerk an.
9. **A.** Der Vollduplex-Modus erlaubt Netzwerkkarten das gleichzeitige Senden und Empfangen von Daten.
10. **D.** Viele Techniker bezeichnen einen Kabeltester als Fox and Hound, dem Namen eines verbreiteten Kabeltester-Modells.

Drahtlose Netzwerke 20

Themen in diesem Kapitel:

- Komponenten drahtloser Netzwerke
- Erörterung drahtloser Netzwerkstandards
- Drahtlose Netzwerke installieren und konfigurieren
- Problembehebung bei drahtlosen Netzwerken

Drahtlose Netzwerke werden zwar bereits seit vielen Jahren verbreitet genutzt, aber im Gegensatz zu kabelgebundenen Netzwerken wissen viele Leute nicht so richtig, wie drahtlose Netzwerke funktionieren. Teilweise könnte dies daran liegen, dass einfache drahtlose Netzwerke derart preiswert und leicht zu konfigurieren sind, dass sich die meisten Benutzer und Techniker nie fragen, *wie* sie eigentlich funktionieren. Die Möglichkeit, ohne Kabel und den damit einhergehenden Kabelsalat auszukommen und sich einfach nur verbinden zu können, ist wohl ungeheuer reizvoll. Das fehlende Verständnis kann problematisch werden, wenn bei drahtlosen Netzwerken Fehler zu beheben sind. Deshalb sollten wir das ändern und uns eingehend mit drahtlosen Netzwerken befassen.

Geschichte und Konzepte

20.1 Drahtlose Netzwerkkomponenten

Statt allen möglichen Kabeln zwischen den Netzwerkknoten verwenden WLANs entweder Funkwellen oder Infrarotlicht, um miteinander zu kommunizieren. In der Vergangenheit kamen und gingen unterschiedliche Arten von drahtlosen Netzwerken. Die heutigen mit Funkwellen arbeitenden drahtlosen Netzwerke basieren auf dem drahtlosen Ethernet-Standard *IEEE 802.11* (mit der Marketing-Bezeichnung »Wi-Fi«) und auf Bluetooth-Technologien. Mit Infrarotlicht arbeitende Netzwerke beschränken sich auf jene, die das *IrDA*-Protokoll (*Infrared Data Association*) verwenden. Die Mobilfunkunternehmen spielen in diesem Bereich natürlich auch eine große Rolle und bieten den Internetzugang über das Mobiltelefonnetz an.

Drahtlose Netzwerkfunktionen der einen oder anderen Art finden Sie in vielen modernen Rechnern. *Infrarot-Transceiver* zählten viele Jahre lang bei tragbaren Computern und hochwertigen Druckern oft zur Standardausstattung, sind bei aktuellen Geräten aber nicht mehr vorhanden, weil es leistungsfähigere Lösungen gibt. Abbildung 20.1 zeigt die Infrarot-Transceiver eines älteren Laptops und eines PDAs, dem Vorgänger des Smartphones. Die Infrarotschnittstelle wurde zur Datenübertragung zwischen in der Nähe befindlichen Geräten benutzt. Heutzutage dient die Infrarotschnittstelle des Smartphones vornehmlich dazu, das Gerät als Fernbedienung für Unterhaltungselektronik zu verwenden. Statt der Infrarotschnittstelle sind nun drahtlose Ethernet- und Bluetooth-Komponenten fest in die Geräte integriert oder lassen sich leicht nachrüsten. Abbildung 20.2 zeigt eine PCI-Steckkarte mit einem Ethernet-WLAN-Adapter. Eingebauter Mobilfunk ist weniger gebräuchlich, findet sich aber in manchen tragbaren Computern (und natürlich in Smartphones). Sie können drahtlose Netzwerkfunktionen auch über externe drahtlose USB-WLAN-Netzwerkadapter nachrüsten (Abbildung 20.3).



Abb. 20.1: Sensoren von Infrarot-Transceivern bei einem PDA und einem Laptop

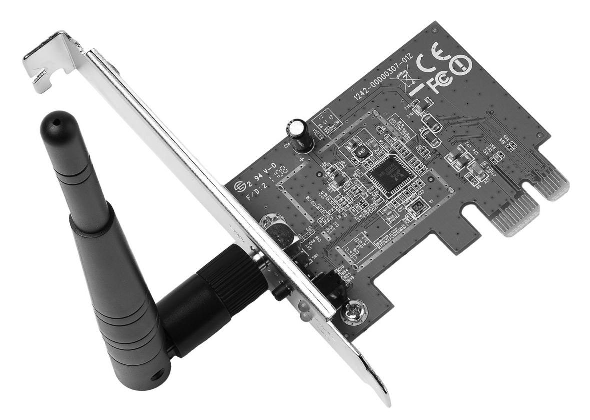


Abb. 20.2: WLAN-Netzadapter als PCIe-Steckkarte



Abb. 20.3: Externer drahtloser USB-Netzwerkadapter

Nicht nur PCs bieten drahtlose Netzwerkfunktionen. Die meisten Smartphones und Tablets bieten integrierte drahtlose Netzwerkfunktionen oder entsprechende Nachrüstoptionen. Abbildung 20.4 zeigt ein Smartphone, das über eine WLAN-Verbindung auf das Internet zugreifen kann.



Abb. 20.4: Smartphone mit drahtlosen Netzwerkfunktionen

Hinweis

Smartphones und Tablets werden in Kapitel 24 ausführlich behandelt.

1001

Um die Fähigkeiten eines drahtlosen Ethernet-Netzwerks zu erweitern und z.B. eine Verbindung zu einem kabelgebundenen Netzwerk herzustellen oder eine schnelle Internetverbindung zu nutzen, benötigen Sie einen drahtlosen *Zugriffspunkt*), einen sogenannten *WAP* (*Wireless Access Point*). Ähnlich wie ein Switch bei kabelgebundenen Ethernet-Rechnern ist ein WAP eine zentrale Verbindungsstelle für drahtlose Netzwerkknoten. Viele WAPs fungieren auch als Switches (für kabelgebundene Rechner) und Internet-Router, wie z.B. der WLAN-Router von Linksys in Abbildung 20.5.



Abb. 20.5: WAP, Switch und WLAN-Router in einem Gerät von Linksys vereint

Die meisten WAPs werden wie üblich über eine normale Steckdose mit Strom versorgt. Einige Geräte, die insbesondere im Firmenumfeld Einsatz finden, verfügen über eine Funktion namens *PoE* (*Power over Ethernet*). Die Stromversorgung findet hier über das Ethernet-Kabel statt. Sie müssen also nur ein einziges Kabel verwenden, um sowohl Netzwerk als auch Stromversorgung durch einen PoE-fähigen Switch bereitzustellen.

Hinweis

PoE wird vornehmlich für WAPs verwendet, aber auch andere Geräte im Netzwerk können diese Funktion nutzen. Da Ethernet-Kabel für gewöhnlich bis zu 100 Meter lang sein dürfen, ist PoE z.B. hervorragend für Überwachungskameras geeignet.

Bei neueren Rechnern und Peripheriegeräten ist die drahtlose Kommunikation via Bluetooth häufig bereits integriert. Wenn das nicht der Fall ist, können Sie Bluetooth über einen externen USB-Bluetooth-Adapter nachrüsten. Alle macOS-Geräte, Desktops und Laptops, sind mit Bluetooth ausgestattet. Am häufigsten wird Bluetooth heutzutage verwendet, um drahtlose Lautsprecher mit einem Smartphone oder Tastaturen mit einem Tablet zu verbinden. Abbildung 20.6 zeigt eine mit einem Bluetooth-fähigen Apple-iPad verbundene Tastatur.

Hinweis

Die drahtlosen Zugriffspunkte werden auch *WAP* (*Wireless Access Point*), *AP* (*Access Point*), *Funkzugriffspunkt* oder *WLAN-Router* genannt.

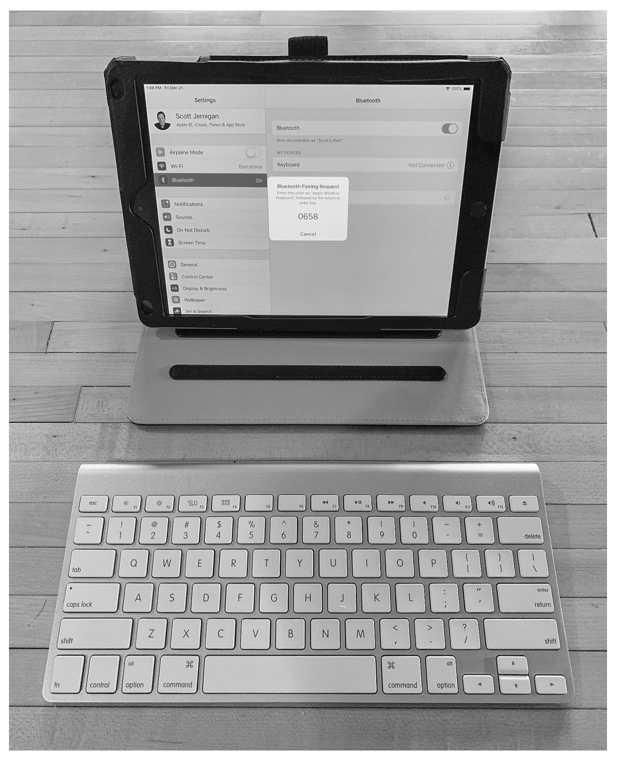


Abb. 20.6: Bluetooth-Tastatur und Tablet

20.1.1 Software für drahtlose Netzwerke

Drahtlose Geräte verwenden dieselben Netzwerkprotokolle und Dienste wie ihre verkabelten Gegenstücke und arbeiten auf der Grundlage des *CSMA/CA*-Zugriffsverfahrens (*Carrier Sense Multiple Access/Collision Avoidance*). »CA« steht für Kollisionsvermeidung (*Collision Avoidance*), einem etwas anderen Standard als die Kollisionserkennung (*Collision Detection*), die in verkabelten Ethernet-Netzwerken verwendet wird. Drahtlose Knoten hören nämlich das drahtlose Medium ab, um festzustellen, ob gerade ein anderer Knoten Daten überträgt. Wenn das der Fall ist, dann warten sie eine zufällige Zeitspanne ab und versuchen dann erneut, Daten zu übertragen. Bis hierhin entspricht das Verfahren genau dem kabelgebundener Ethernet-Netzwerke. Da die Erkennung von Datenkollisionen für drahtlose Knoten aber schwieriger ist, kann optional das *RTS/CTS-Protokoll* (*Request to Send/Clear to Send*) verwendet werden. Wenn es aktiviert ist, dann überträgt ein Knoten, der ein freies drahtloses Medium erkennt und senden will, ein RTS-Paket zum Empfängerknoten. Dieser antwortet mit einem CTS-Paket und teilt dem Senderknoten mit, dass er mit der Übertragung beginnen kann. Wenn Daten übertragen wurden, dann wartet der sendende Knoten auf eine Bestätigung (*ACK – acknowledgment*) des Empfängerknotens, bevor er das nächste Datenpaket überträgt. Das ist zwar sehr elegant, aber dadurch führt RTS/CTS zu einem deutlichen Verwaltungsaufwand, der die Leistung beeinträchtigen kann.

Bei der Konfiguration der Software für drahtlose Netzwerke müssen Sie nur wenig tun. Drahtlose Netzwerkadapter entsprechen dem PnP-Standard, sodass sie von allen modernen Windows- oder macOS-Versionen bei ihrer Installation sofort erkannt werden. Möglicherweise werden Sie dann zum Einlegen eines Datenträgers mit Hardwaretreibern aufgefordert. Es wird allerdings ein Hilfsprogramm benötigt, mit dem Parameter wie der Netzwerkname eingestellt werden können.

Die aktuellen Windows- und macOS-Versionen enthalten integrierte Hilfsprogramme zur Konfiguration dieser Einstellungen (Abbildung 20.7), aber einige Hersteller von drahtlosen Netzwerkadaptern

liefern dennoch Konfigurationsprogramme mit. Mit diesem Hilfsprogramm können Sie die Verbindungsqualität und die Signalstärke ermitteln, den drahtlosen Netzwerkmodus konfigurieren (der nachfolgend beschrieben wird), die Verschlüsselung aktivieren, Energieoptionen einstellen usw.



Abb. 20.7: Programm zur WLAN-Konfiguration in macOS

20.1.2 Drahtlose Netzwerkmodi

Das einfachste drahtlose Netzwerk besteht aus zwei oder mehr Rechnern oder Geräten, die direkt (ohne Kabel oder andere vermittelnde Hardware) miteinander kommunizieren. Komplexere drahtlose Netzwerke nutzen einen WAP, um die drahtlose Kommunikation zu zentralisieren und drahtlose Netzwerksegmente mit kabelgestützten Netzwerksegmenten zu verbinden. Diese beiden verschiedenen Verfahren werden Ad-hoc- und Infrastruktur-Modus genannt.

Ad-hoc-Modus

Der *Ad-hoc-Modus* wird manchmal auch *Peer-to-Peer-Modus* genannt. Dabei befinden sich alle drahtlosen Knoten in einem dezentralisierten und frei zugänglichen Modus untereinander in direktem Kontakt (Abbildung 20.8). Zwei oder mehr im Ad-hoc-Modus kommunizierende drahtlose Knoten bilden eine Gruppe (*IBSS – Independent Basic Service Set*). Netzwerke lassen sich im Ad-hoc-Modus einfacher als im Infrastruktur-Modus konfigurieren und eignen sich für kleine Rechnergruppen (weniger als etwa ein Dutzend), die Dateien übertragen oder Drucker gemeinsam nutzen möchten. Ad-hoc-Netzwerke sind auch gut für temporäre Netzwerke geeignet, wie z.B. Studiengruppen oder Geschäftstreffen.

Hinweis

Mit Windows 8.1 hat Microsoft die standardmäßige Unterstützung von Ad-hoc-Netzwerken eingestellt. Wenn Sie diese verwenden möchten, müssen Sie die vollständige Unterstützung auf der Kommandozeile aktivieren.

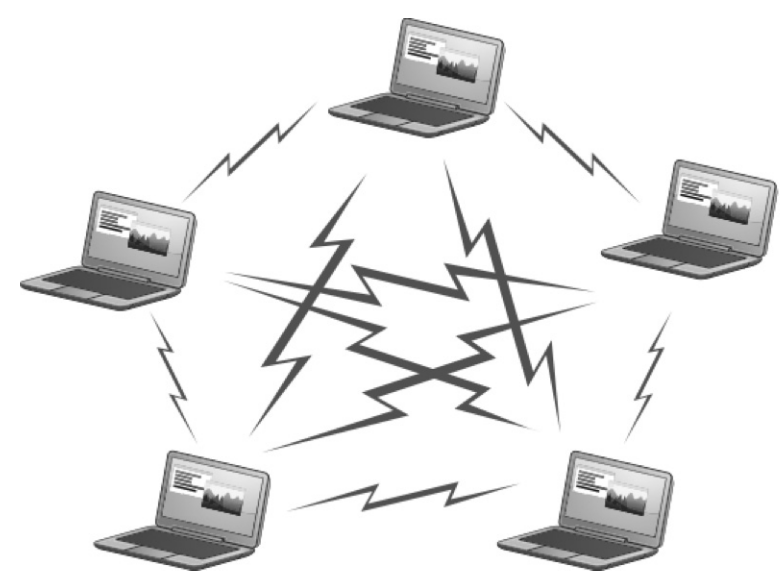


Abb. 20.8: Drahtloses Netzwerk im Ad-hoc-Modus

Infrastruktur-Modus

Im *Infrastruktur-Modus* arbeitende drahtlose Netzwerke benutzen mindestens einen WAP, um die drahtlosen Netzwerkknoten mit einem verkabelten Netzwerksegment zu verbinden (Abbildung 20.9). Ein einzelner WAP, der für einen bestimmten Bereich zuständig ist, wird *BSS* (*Basic Service Set*) genannt. Der abgedeckte Bereich lässt sich durch das Hinzufügen weiterer WAPs erweitern. Entsprechend ist dann von *EBSS* (*Extended Basic Service Set*) die Rede.

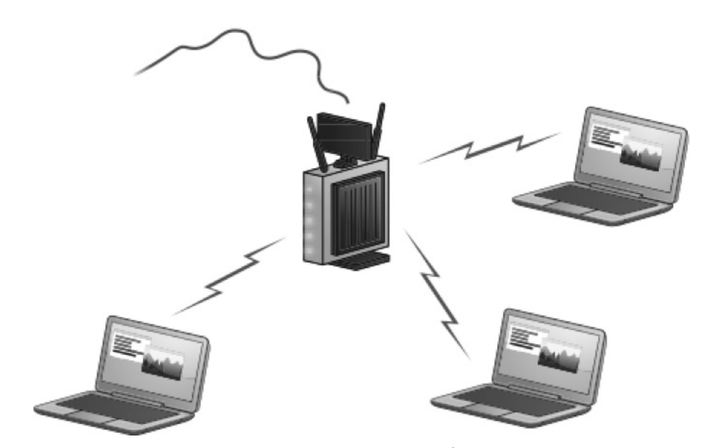


Abb. 20.9: Drahtloses Netzwerk im Infrastruktur-Modus

Wichtig

In der CompTIA A+-Zertifizierungsprüfung wird sehr wahrscheinlich nach den angemessenen Umgebungen für Infrastruktur- und Ad-hoc-Modus gefragt. Der Infrastruktur-Modus ist gängige Praxis, in manchen Situationen kann aber auch ein kurzfristig improvisiertes Ad-hoc-Netzwerk sinnvoll sein. Ansonsten werden Sie Ad-hoc-Netzwerken heutzutage kaum noch begegnen.

Im Infrastruktur-Modus arbeitende drahtlose Netzwerke erfordern mehr Planung und sind schwieriger zu konfigurieren als Netzwerke im Ad-hoc-Modus, bieten aber mehr Kontrolle über die Arbeitsweise des Netzwerks. Der Infrastruktur-Modus eignet sich besser für Unternehmensnetze, in denen dedizierte Ressourcen (z.B. Internetzugang und zentrale Datenbanken) gemeinsam genutzt werden. Er wird häufig in *SOHO*-Netzwerken (*Small Office/Home Office*) eingesetzt und die WAPs in solchen Umgebungen werden daher als SOHO-WAP oder SOHO-Router bezeichnet.

Wichtig

Viele Hersteller bieten Geräte für eine Hybrid-Netzwerktopologie an, bei der die meisten Geräte mit einem drahtlosen sogenannten Mesh-Netzwerk verbunden sind, das jedoch auch einige kabelgebundene Geräte umfasst. Das entscheidende Merkmal eines solchen WMN (*Wireless Mesh Network*) ist, dass die Netzknoten wie Router funktionieren und den Datenverkehr weiterleiten, nur eben drahtlos.

In der Praxis sind WMNs tendenziell »statischer« als normale Ad-hoc-Netzwerke. Damit ist gemeint, dass die Geräte dem Netzwerk nicht so schnell beitreten oder es wieder verlassen. Zudem gibt es auch kabelgebundene Netzwerkknoten. WMNs werden derzeit in speziellen Umgebungen verwendet, beispielsweise bei Außeneinsätzen des Militärs oder bei Google-Home-Geräten.

1002

20.1.3 Sicherheit in drahtlosen Netzwerken

Einer der häufigsten Einwände gegen drahtlose Netzwerke sind deren schwache Sicherheitsfunktionen, wenngleich die Industrie in dieser Hinsicht in den letzten Jahren doch deutliche Fortschritte gemacht hat. Schließlich werden die Datenpakete über Funk und nicht geschützt über die Leitungen eines Netzwerkkabels übertragen. Was soll also skrupellose Leute mit der richtigen Ausrüstung davon abhalten, die übertragenen Datenpakete abzufangen und die Daten zu lesen? Früher mussten Sie sich oft nur in die Reichweite des WAPs begeben und ein drahtloses Gerät einschalten, um auf ein drahtloses Netzwerk zugreifen zu können. Heutzutage sind kaum noch versehentlich offen zugängliche Netzwerke zu finden, da die Hersteller vernünftigerweise bestimmte Sicherheitseinstellung als Standard vorgeben. Dennoch bereiten diese gut gemeinten Vorgaben manchmal Schwierigkeiten, daher ist es wichtig, einen kritischen Blick auf die Einstellungen neuer Geräte zu werfen.

Drahtlose Netzwerke verwenden drei Verfahren, um den Zugriff auf das Netzwerk selbst und die übertragenen Daten zu schützen: MAC-Adressfilter, Authentifizierung und Datenverschlüsselung. Doch bevor irgendjemand mit den Sicherheitsfunktionen in Berührung kommt, können wir einige vorbeugende Maßnahmen zum Senken der Wahrscheinlichkeit treffen, dass unser drahtloses Netzwerk überhaupt angegriffen wird. Diese Maßnahmen sehen wir uns nun an und danach betrachten wir die Methoden, mit denen das Netzwerk selbst geschützt werden kann.

SSID

Der *SSID*-Parameter (*Service Set Identifier* bzw. *Netzwerkname*) legt den Namen des drahtlosen Netzwerks fest. Nun ist es für gewöhnlich ja gewollt, dass ein drahtloses Netzwerk auffindbar ist, daher sind WAPs meistens so konfiguriert, dass sie ihr Vorhandensein kundtun, indem sie regelmäßig mit maximaler Sendeleistung ihre SSID übertragen. Das ist sehr praktisch, wenn mehrere drahtlose Netzwerke im selben Bereich arbeiten, aber die Standard-SSID enthält auch wichtige Hinweise auf den Hersteller (und eventuell sogar das Modell) des Zugriffspunkts.

Ändern Sie immer sofort die SSID und auch das Kennwort. Die Konfiguration einer eigenen SSID und eines Kennworts ist das Mindeste, was Sie zur Absicherung eines drahtlosen Netzwerks erledigen sollten. Die vorkonfigurierten Netzwerknamen und Kennwörter älterer Geräte sind wohlbekannt und online zugänglich. Neuere Modelle besitzen jeweils eindeutige SSIDs und Kennwörter, aber dennoch

könnte die Standard-SSID Auskunft über Ihre Hardware geben – und die Regel zum Erzeugen des eindeutigen Kennworts (z.B. anhand der MAC-Adresse) könnte leicht herauszufinden sein.

Die Standardeinstellungen sollen die Einrichtung drahtloser Netzwerke möglichst vereinfachen, sorgen aber spätestens dann für enorme Sicherheitslücken, wenn sich auf engem Bereich viele drahtlose Netzwerke überlappen. Alle drahtlosen Netzwerkknoten und Zugriffspunkte innerhalb eines drahtlosen Netzwerks müssen mit derselben eindeutigen SSID konfiguriert werden. Die SSID wird dann in den Header aller übertragenen Datenpakete im drahtlosen Netzwerk eingebunden. Datenpakete mit falscher SSID werden zurückgewiesen. Denken Sie bei der Auswahl der SSID auch darüber nach, ob die Bezeichnung das Netzwerk nach einem lohnenden Ziel aussehen lässt, und achten Sie darauf, dass der Name keine Informationen enthält, die es einem Angreifer ermöglichen könnten, auf das Gerät selbst oder auf das Netzwerk zuzugreifen.

Ein weiterer Trick, dem man bei drahtlosen Netzwerken häufig begegnet, besteht darin, die SSID nicht offen zu übertragen. Damit können Unberechtigte nicht ganz so leicht auf das Netzwerk zugreifen, weil der Name in der Liste der umliegenden Netzwerke auf den meisten Geräten dann nicht erscheint.

In der Praxis können allerdings schon einfache Programme zum Scannen drahtloser Netzwerke den Namen eines »unbekannten« Netzes herausfinden. Die offene Übertragung der SSID zu unterbinden, erschwert es vor allem legitimen Benutzern, sich mit dem Netzwerk zu verbinden, hält böse Buben jedoch keineswegs fern – höchstens in einer Frage der CompTIA A+-Zertifizierungsprüfung.

Wichtig

Die CompTIA nennt das Ändern der Standard-SSID und das Unterbinden der offenen SSID-Übertragung als Schritte zur Absicherung eines drahtlosen Netzwerks. Geschützt wird das Netzwerk in der Praxis dadurch nicht. Sie müssen vielmehr sichere Protokolle für die Datenübertragung konfigurieren.

Platzierung des WAPs und Sendeleistung

Beachten Sie bei der Einrichtung eines drahtlosen Netzwerks die räumlichen Gegebenheiten. Sie können das Risiko vermindern, indem Sie Ihr Netzwerk vor der Außenwelt verbergen. Wenn der WAP eine omnidirektionale Antenne besitzt (die Signale in alle Richtungen abstrahlt und aus allen Richtungen empfängt), sollten Sie ihn möglichst im Zentrum Ihres Hauses oder Büros platzieren. Je näher sich der WAP an einer Außenwand befindet, umso weiter können Personen außerhalb Ihres Hauses oder Büros entfernt sein und dennoch Ihr drahtloses Netzwerk ausfindig machen.

Viele Geräte ermöglichen es auch, die Sendeleistung der Antenne zu regeln. Senken Sie die Sendeleistung so weit ab, dass innerhalb Ihres Hauses oder Büros stabiler Empfang möglich ist, außerhalb jedoch nicht. Damit ist allerdings ein gewisses Herumprobieren verbunden.

Wichtig

Denken Sie daran, den WAP auch vor physischem Zugriff zu schützen. Die meisten WAPs besitzen neben der drahtlosen Funktionalität auch Ethernet-Anschlüsse, die nicht kennwortgeschützt oder verschlüsselt sind. Platzieren Sie den WAP an einem Ort, an dem er vor Spitzbuben sicher ist.

MAC-Adressfilter

Die meisten WAPs unterstützen auch das Filtern von MAC-Adressen. Bei diesem Verfahren können Sie den Zugang zum drahtlosen Netzwerk auf bestimmte physische, fest verdrahtete Adressen drahtloser Netzwerkadapter beschränken. Der *MAC-Adressfilter* bietet ein praktisches Verfahren zum Erstellen von Listen zulässiger Benutzer und kann den Zugang zum drahtlosen Netzwerk strikt beschränken. Am besten funktioniert das, wenn es nur wenige Benutzer gibt. Im WAP wird eine Tabelle mit den MAC-Adressen gespeichert, die auf das drahtlose Netzwerk zugreifen dürfen. Alle Datenpakete, die nicht eine der in dieser Tabelle aufgeführten MAC-Adressen enthalten, werden zurückgewiesen.

Hinweis

MAC-Adressfilter scheinen auf den ersten Blick sehr sicher zu sein, sie sind es aber nicht. Ein Angreifer kann spezielle Software verwenden, um die MAC-Adressen von in der Nähe befindlichen Geräten abzuhören, und die Adresse eines zugelassenen Clients fälschen (*Spoofing*).

Drahtlose Verschlüsselungsprotokolle und Authentifizierungsverfahren

Drahtlose Verschlüsselungsprotokolle stellen zum Schutz drahtloser Netzwerke Authentifizierung und Verschlüsselung bereit. Drahtlose Netzwerke bieten tolle Verbindungsmöglichkeiten, sind aber auch verlockende Ziele. Die Entwickler haben große Anstrengungen unternommen, um Technikern die nötigen Werkzeuge zum Schutz der drahtlosen Clients und der Kommunikation bereitzustellen. Die drahtlose Authentifizierung bewirkt dasselbe wie die drahtgebundene. Sie ermöglicht es dem System, die Anmeldedaten eines Benutzers zu überprüfen und Zugriff auf das Netzwerk zu gewähren oder zu verweigern. Die Verschlüsselung würfelt die per Funk übertragenen Daten durcheinander und schützt so die Kommunikation zwischen Benutzern.

In diesem Abschnitt geht es um die verschiedenen Generationen drahtloser Verschlüsselungsprotokolle. Wir betrachten typische Authentifizierungsverfahren und sehen uns zum Schluss eine einfache benutzerfreundliche Lösung an. (Im nachfolgenden Abschnitt *Infrastruktur-Modus* finden Sie Details zu Authentifizierungsverfahren im Firmenumfeld.)

WEP Schon sehr früh führten die Entwickler zum Schutz der im WLAN übertragenen Daten das *WEP*-Protokoll (*Wired Equivalent Privacy*) ein. WEP verwendet standardmäßige eine 40-Bit-Verschlüsselung für die Datenpakete. Viele Anbieter unterstützen auch eine 104-Bit-Verschlüsselung. Beachten Sie, dass zwar oft mit 128-Bit-Verschlüsselung geworben wird, dass dabei aber eigentlich 104-Bit-Schlüssel verwendet werden. Leider enthält die WEP-Verschlüsselung eine Lücke, durch die sie leicht zu knacken ist. WEP ist zwar besser als gar keine Verschlüsselung, kann aber gewiefte Angreifer mit den nötigen Kenntnissen nicht aussperren.

Wichtig ist es anzumerken, dass zur Verschlüsselung des gesamten WEP-Datenverkehrs eines Netzwerks derselbe Schlüssel verwendet wird. Der Datenverkehr eines Benutzers ist anderen Benutzern desselben Netzwerks also zugänglich. Eine echte und vollständige Verschlüsselung, die für jeden Client einen eigenen Schlüssel verwendet, erreichen Sie erst mit WPA oder WPA2.

WPA *WPA* (*Wi-Fi Protected Access*) vermeidet die Schwächen von WEP und stellt eine Art Aktualisierung des WEP-Sicherheitsprotokolls dar. WPA verwendet *TKIP* (*Temporal Key Integrity Protocol*) und nutzt für die Verschlüsselung jedes Datenpakets einen neuen Schlüssel. Dadurch ist es vor vielen Angriffen geschützt, die WEP so verwundbar machen. TKIP ist aber auch schon veraltet, da dieses Protokoll mit eigenen Problemen zu kämpfen hat. WPA bietet Sicherheitsfunktionen, wie z.B. eine Integritätsprüfung verschlüsselter Daten und eine Benutzerauthentifizierung über den Industriestandard *EAP* (*Extensible Authentication Protocol*). Der Einsatz von EAP ist deutlich sicherer als die WEP-Verschlüsselung, aber selbst mit diesen Erweiterungen war WPA lediglich als vorübergehende Sicherheitslösung bis zur Fertigstellung und Implementierung des IEEE-802.11i-Sicherheitsstandards WPA2 gedacht.

WPA2 Heutzutage unterstützen Linux, macOS und Windows den vollständigen IEEE-802.11i-Standard, der auch als *WPA2* (*Wi-Fi Protected Access 2*) bekannt ist, um drahtlose Netzwerke zu sichern. Neben anderen Verbesserungen verwendet WPA2 *AES* (*Advanced Encryption Standard*) zum Schutz der drahtlosen Umgebung. Wenn Sie WPA2 noch nicht verwenden, dann sollten Sie die entsprechenden Upgrades schnell nachholen. Alle aktuellen WAPs und Endgeräte unterstützen WPA2 und die meisten Router sind abwärtskompatibel, um die wenigen Geräte zu unterstützen, die noch die erste WPA-Generation verwenden. Das kann beim Einsatz älterer Netzwerkadapter oder WAPs erforderlich sein, weil die alte Hardware WPA2 nicht verwenden kann (wie beispielsweise die ersten Geräte, die den 802.11b-Standard implementierten). Jüngere Modelle solcher Geräte unterstützen AES und WPA2.

WPA3 Anfang 2018 wurde der Nachfolger von WPA2 angekündigt (natürlich WPA3!). Die Unterstützung von WPA3 ist noch in Arbeit (für Windows 10 wird irgendwann im Jahr 2019 damit gerechnet), aber das Protokoll sollte in den kommenden Jahren immer gebräuchlicher werden. WPA3 behebt einige der Probleme bei der Sicherheit und der Verwendbarkeit, unter anderem die Verschlüsselung der Daten zum Schutz der Benutzer offener (öffentlich zugänglicher) Netzwerke.

Wichtig

WPA3 hat es dieses Mal noch nicht in die Lernziele der CompTIA geschafft. Dieses Kapitel und die Prüfung betrachten also WPA2 als letzte Generation der WLAN-Sicherheit. Wenn Sie Realist sind und kein Zeitreisender aus den Jahren vor 2019, sollten Sie die Software- und Hardware-Unterstützung für WPA3 im Auge behalten und WPA3-kompatible Geräte empfehlen, sobald diese verfügbar sind. Implementieren Sie, sofern möglich, WPA3-Netzwerke und deaktivieren Sie WPA2 allmählich, wenn alle von Ihnen betreuten Geräte WPA3-kompatibel sind.

WPS Die meisten Techniker können drahtlose Netzwerke mit geschlossenen Augen konfigurieren, aber normalen Anwendern ist der Gedanke an Kennwörter und Verschlüsselung oft nicht ganz geheuer. Die meisten Leute schließen einfach nur den Router an und freuen sich des Lebens. Um die allgemeine Sicherheit drahtloser Netzwerke zu erhöhen, wurde daher *WPS* (*Wi-Fi Protected Setup*) entwickelt, ein Standard, den die meisten WAPs und WLAN-Geräte unterstützen und der die Konfiguration sicherer Netzwerke erleichtern soll.

Bei WPS gibt es zwei Arbeitsweisen. Einige Geräte, wie der Router in Abbildung 20.10, verwenden eine Taste, andere hingegen ein Kennwort oder einen Code.



Abb. 20.10: e2500-Router mit WPS-Taste

Nehmen wir an, Sie möchten einen WPS-fähigen drahtlosen Drucker mit einem ebenfalls WPS-fähigen WAP verbinden. Zunächst betätigen Sie dann einen Moment lang die WPS-Taste am Drucker (für gewöhnlich zwei Sekunden). Dadurch wird ein Zeitfenster geöffnet (normalerweise zwei Minuten), innerhalb dessen Sie den WPS-Knopf am WAP drücken müssen. Auf diese Weise wird automatisch eine sichere Verbindung konfiguriert.

Einige Geräte erlauben auch die Verwendung eines Codes. Bei WSP-fähigen WAPs ist dieser achtstellige numerische Code irgendwo auf dem Gehäuse angebracht. Um auf den WAP zuzugreifen, geben Sie diesen Code in Ihrem Betriebssystem ein, als ob Sie ein WPA/WPA2-Kennwort verwenden würden. Schon sind Sie mit dem Netzwerk verbunden.

Bedauerlicherweise besitzt WPS eine Sicherheitslücke. Ein Hacker kann ein Programm benutzen, um verschiedene Werte für den achtstelligen Code auszuprobieren. Durch die Methode, mit der dieser Code erzeugt wird, ist er leicht zu erraten. Wenn auf Ihrem WAP WPS aktiviert ist, sind Sie angreifbar. Es gibt nur eine Möglichkeit, einen solchen Hack zu verhindern: WPS deaktivieren. Eine Anleitung dazu sollten Sie auf der Website des Herstellers finden.

1001

20.1.4 Geschwindigkeit und Reichweite

Der Datendurchsatz drahtloser Netzwerke hängt von mehreren Faktoren ab. Zunächst von dem von den drahtlosen Geräten verwendeten Standard. Je nach eingesetztem Standard liegt der Datendurchsatz zwischen mäßigen 2 Mbps und flotten 1 Gbps oder mehr. Ein weiterer Faktor, der die Geschwindigkeit beeinflusst, ist die Entfernung zwischen den drahtlosen Knoten (oder zwischen den drahtlosen Knoten und dem zentralen Zugriffspunkt). Drahtlose Geräte handeln die für die Kommunikation zu verwendende Spitzengeschwindigkeit dynamisch aus, ohne dass dabei sonderlich viele Datenpakete ungültig werden. Mit zunehmender Entfernung nimmt die Geschwindigkeit ab, sodass der maximale Durchsatz nur bei kurzer Entfernung erreicht werden kann (weniger als etwa zehn Meter). In den Grenzbereichen der Reichweite kann die Geschwindigkeit bis auf ca. 1 Mbps abfallen, bevor die Verbindung komplett abreißt.

Die Geschwindigkeit und die Reichweite werden auch durch Störungen durch andere drahtlose Geräte, die in demselben Frequenzbereich arbeiten (z.B. Schnurlostelefon oder Babyfon), und massive Gegenstände beeinflusst. Solche Funklöcher treten auf, wenn die Signale zwischen den drahtlosen Netzwerkknoten blockiert werden. Große Elektrogeräte, wie z.B. Kühlschränke, können die Funksignale drahtloser Netzwerke *äußerst* wirksam unterbrechen! Weitere mögliche Störenfriede sind elektrische Sicherungskästen, Rohrleitungen aus Metall, Klimaanlagen usw.

Hinweis

Die Geschwindigkeit und die Signalstärke Ihres drahtlosen Netzwerks können Sie bei den Eigenschaften des drahtlosen Netzwerkadapters ablesen. Öffnen Sie dazu in der Systemsteuerung das Applet NETZWERK- UND FREIGABECENTER und klicken Sie auf ADAPTEREINSTELLUNGEN ÄNDERN. Doppelklicken Sie dann auf den drahtlosen Netzwerkadapter, um das Dialogfeld STATUS anzuzeigen.

Die Reichweite drahtloser Netzwerke lässt sich nur schwer definieren. Meist finden Sie Angaben wie »ca. 50 Meter« oder »etwa 100 Meter«. Das liegt einfach daran, dass die Reichweite ähnlich wie der Datendurchsatz stark von Umweltfaktoren beeinflusst wird. Interferenzen mit anderen drahtlosen Geräten oder massive Objekte können sich auf die Reichweite auswirken. Die Angaben zur maximalen Reichweite im nächsten Abschnitt entsprechen daher denen der Hersteller und sind theoretische Maximalwerte. Im praktischen Einsatz werden diese Werte nur unter Idealbedingungen erreicht. Meist liegt die Reichweite in der Praxis nur bei etwa der Hälfte der angegebenen Werte.

Die Reichweite lässt sich mit einigen Verfahren erhöhen. Zunächst einmal können Sie mehrere WAPs installieren, sodass man zwischen den verschiedenen Deckungsbereichen der WAPs wechseln kann und damit ein EBSS einrichtet. Oder Sie können bessere Antennen verwenden, um die Signalstärke zu erhöhen. Und wenn das noch nicht reicht, können Sie Signalverstärker (Repeater) installieren, die WLAN-Signale empfangen und weiterleiten.

Wichtig

Bereiten Sie sich auf Fragen in den CompTIA A+-Prüfungen vor, die sich auf Faktoren beziehen, die die drahtlose Kommunikation, deren Reichweite sowie deren Geschwindigkeit beeinträchtigen können.

20.2 Drahtlose Netzwerkstandards

Die Welt der drahtlosen Kommunikation ist heutzutage von Funktechnologien geprägt, insbesondere durch den IEEE-802.11-Standard, aber auch Infrarot, Bluetooth und Mobilfunk haben ihren Platz. Um die drahtlose Netzwerktechnologie besser verstehen zu können, werden wir nun kurz die hier verwendeten Standards betrachten.

Hinweis

Funkwellen sind der Teil des elektromagnetischen Spektrums, der zur drahtlosen Kommunikation verwendet wird.

20.2.1 Drahtlose Netzwerke nach IEEE 802.11

Der drahtlose Ethernet-Standard *IEEE 802.11*, der auch unter dem Namen *Wi-Fi* bekannt ist, definiert Verfahren der Datenübertragung mittels *Frequenzspreizung* von Funkwellen (*Spread-Spectrum*). Beim Frequenzspreizungsverfahren werden die Daten in kleinen Blöcken über die verschiedenen verfügbaren Frequenzen innerhalb eines bestimmten Frequenzbereichs verteilt übertragen.

Hinweis

Wi-Fi und andere drahtlose Kommunikationstechnologien verwenden Frequenzen, die zum sogenannten ISM-Frequenzbereich (*Industrial, Science and Medical*) gehören. Dadurch kann es zu Interferenzen mit anderen Geräten kommen, wie beispielsweise Mikrowellengeräte oder Babyfons.

Alle der auf 802.11 basierenden drahtlosen Technologien verwenden zum Senden und Empfangen eines von zwei frei zugänglichen Frequenzbändern. Dabei handelt es sich um zusammenhängende Frequenzbereiche, die weiter in sogenannte *Kanäle* unterteilt werden. Der ursprüngliche 802.11-Standard wurde mit der Zeit um die Varianten 802.11a, 802.11b, 802.11g, 802.11n und 802.11ac erweitert, die in drahtlosen Netzwerken verwendet werden. Sämtliche 802.11-Varianten verwenden eines der beiden Bänder, nur 802.11n kann auch beide benutzen. Keine Sorge, ich werde das für Sie gleich noch genauer aufschlüsseln.

Hinweis

Wi-Fi ist heute der bei Weitem verbreitetste drahtlose Netzwerktyp. Drahtlose Netzwerke werden nicht nur in vielen Kleinunternehmen und Wohnungen, sondern auch an öffentlichen Plätzen (z.B. Cafés und Bibliotheken) eingesetzt, die ebenfalls den Internetzugang über drahtlose Netzwerke anbieten.

Neuere drahtlose Geräte können mit älteren drahtlosen Geräten kommunizieren. Wenn Sie also einen 802.11n-WAP verwenden, dann kann dieser auch von Ihren 802.11g-Geräten benutzt werden. Die Ausnahme bildet 802.11a, das ein 5-GHz-Frequenzband benötigt. Damit sind also nur WAPs nach einem der Standards 802.11ac oder 802.11ac (Dualband) kompatibel. In den folgenden Absätzen werden die wichtigen Spezifikationen der verschiedenen 802.11-basierten drahtlosen Netzwerkstandards beschrieben.

802.11a Ungeachtet der Kennung »a« dieser Erweiterung des 802.11-Standards kam 802.11a eigentlich erst *nach* 802.11b auf den Markt. 802.11a unterscheidet sich von den anderen 802.11-basierten Standards deutlich. Zunächst nutzt es mit 5 GHz einen anderen Frequenzbereich. Dadurch werden Geräte, die mit diesem Standard arbeiten, weniger durch andere Geräte gestört, die im selben Frequenzbereich operieren. 802.11a bietet mit 54 Mbps auch einen deutlich besseren Datendurchsatz als

802.11 und 802.11b, auch wenn die tatsächliche Datenrate bei normaler Nutzung nicht über 25 Mbps liegt. Die maximal erreichbare Reichweite liegt zwar bei ca. 50 Metern, wird aber im typischen Büroumfeld nur selten erreicht. Trotz der höheren Geschwindigkeit und der geringeren Störanfälligkeit ist 802.11a im PC-Bereich weniger verbreitet als einige der nachfolgenden 802.1-Versionen.

802.11b 802.11b war der erste im Bereich drahtloser Netzwerke weitverbreitete Standard. Der Standard unterstützt einen Datendurchsatz von maximal 11 Mbps (bei einem tatsächlichen mittleren Durchsatz von 4 bis 6 Mbps), liegt damit etwa gleichauf mit den alten verdrahteten 10Base-T-Netzwerken und bietet unter Idealbedingungen eine maximale Reichweite von ca. 100 Metern. Im typischen Büroumfeld ist die maximale Reichweite geringer. Der wesentliche Nachteil von 802.11b besteht darin, dass es mit dem 2,4-GHz-Band eine bereits reichlich überlastete Frequenz benutzt (Babyfone, Garagentoröffner, Mikrowellen), wodurch leicht Störungen durch andere drahtlose Geräte auftreten können.

802.11g Der 802.11g-Standard erschien 2003, übernahm die besten Eigenschaften von 802.11a und 802.11b und vereinte sie in einem einzigen Standard. 802.11g bietet Datentransferraten von maximal 54 Mbps (wie 802.11a) bei der größeren Reichweite von ca. 100 Metern (wie 802.11b). Wichtiger ist aber, dass 802.11g abwärtskompatibel mit 802.11b ist, sodass ein 802.11g-WAP sowohl 802.11b- als auch 802.11g-Knoten unterstützt.

802.11n Mit dem 802.11n-Standard gehen einige Verbesserungen in Wi-Fi-Netzwerken einher, zu denen höhere Geschwindigkeiten und neue Antennentechnologien zählen.

Um eine Funktion zu unterstützen, die *MIMO* (*Multiple In/Multiple Out*) genannt wird und mit deren Hilfe Geräte mehrere Verbindungen gleichzeitig aufbauen können, fordert die 802.11n-Spezifikation, dass mit Ausnahme von Handheld-Geräten alle Geräte mehrere Antennen benutzen. Mit bis zu vier Antennen können 802.11n-Geräte erstaunliche Geschwindigkeiten erreichen. Der offizielle Standard unterstützt Datenraten von bis zu 600 Mbps, die Werte im praktischen Einsatz liegen aber erheblich niedriger (etwa 100 MBps bei einer Entfernung von 100 Metern).

Hinweis

Da die meisten Smartphones sowohl Mobilfunknetze als auch drahtlose Netzwerke nach einem der 802.11x-Standards unterstützen, können sie als Bridge eingesetzt werden. Dank interner Hilfsprogramme oder einer App können Sie Ihr Smartphone als WAP konfigurieren, der die via Mobilfunk hergestellte Internetverbindung per WLAN weiterreicht. Wenn man ein Smartphone als WAP einsetzt, nennt man es einen *Hotspot*. Der eigentliche Vorgang, die Internetverbindung weiterzugeben, wird als *Tethering* (zu Deutsch etwa »Anbindung«) bezeichnet. In den Kapiteln 21 und 24 gehe ich näher darauf ein.

Viele 802.11n-WAPs nutzen mit der *Sendestrahlsteuerung* (*TxBF – Transmit Beamforming*) eine Mehrantennentechnologie, mit der sich Funklöcher besser vermeiden bzw. abschwächen lassen. Wenn ein WAP einen Client erkennt, dann passt die Antenne das Funksignal zwecks Optimierung an.

Wie bei 802.11g können auch 802.11n-WAPs das 2,4-GHz-Band nutzen und ältere, langsamere 802.11b/g-Geräte unterstützen. 802.11n-Geräte können aber auch den leistungsfähigeren sogenannten *Dualband*-Modus unterstützen. Dazu werden fortschrittlichere (und teurere) WAPs benötigt, die gleichzeitig die beiden Frequenzen 5 und 2,4 GHz nutzen. Teilweise unterstützen derartige Geräte nicht nur 802.11b/g, sondern auch 802.11a.

802.11ac Hierbei handelt es sich um die folgerichtige Weiterentwicklung des 802.11n-Standards, der mehrere Streams und eine höhere Bandbreite nutzt und dementsprechend schneller ist. Um die Probleme mit dem stark ausgelasteten 2,4-GHz-Band zu vermeiden, nutzt 802.11ac das 5-GHz-Band. Die jüngste Version unterstützt darüber hinaus eine neue MIMO-Version, die den Namen *Multiuser MIMO* oder kurz *MU-MIMO* trägt. Durch MU-MIMO ist der WAP in der Lage, Daten an mehrere Benutzer gleichzeitig zu übertragen. Wie 802.11n unterstützt auch 802.11ac den Dualband-Modus. Einige WAPs unterstützen sogar drei Frequenzbänder und nutzen ein zweites 5-GHz-Signal, um mehrere 5-GHz-Verbindungen mit optimaler Geschwindigkeit gleichzeitig aufzubauen.

Wichtig

Zwei Ende 2018 und Anfang 2019 vorgestellte Entwicklungen werden in der CompTIA A+-Prüfung 1001 zwar nicht vorkommen, sie werden in den nächsten Jahren jedoch für Techniker relevant sein. Zum einen die nächste Wi-Fi-Generation mit der Bezeichung *802.11ax*, die 2019 auf den Markt kommt. Die Hersteller haben schon 2017 und 2018 eine Reihe von Prototypen gezeigt. Der Standard bietet höhere Geschwindigkeiten als 802.11ac und verwendet das 2,4- und das 5-GHz-Frequenzband. 802.11ax wird auch als HEW (*High Efficiency Wireless*) bezeichnet.

Zum anderen hat die Wi-Alliance im Oktober 2018 neue Markenbezeichnungen für 802.11n, 802.11ac und 802.11ax angekündigt. Sie lauten WiFi 4, WiFi 5 bzw. WiFi 6. Die Hersteller verwenden diese Namen bereits, rechnen Sie also damit, dass Ihre Kunden sie ebenfalls benutzen.

In Tabelle 20.1 sind die wichtigsten Unterschiede der verschiedenen 802.11-Versionen aufgeführt.

Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Max. Durchsatz	54 Mbps	11 Mbps	54 Mbps	> 100 Mbps	> 1 Gbps
Max. Reichweite	50 Meter	100 Meter	100 Meter	> 100 Meter	> 100 Meter
Frequenzband	5 GHz	2,4 GHz	2,4 GHz	2,4 und 5 GHz	5 GHz
Sicherheit	SSID, MAC-Filterung, Industriestandard: WEP, WPA, WPA2	SSID, MAC-Filterung, Industriestandard: WEP, WPA, WPA2	SSID, MAC-Filterung, Industriestandard: WEP, WPA, WPA2	SSID, MAC-Filterung, Industriestandard: WEP, WPA, WPA2	SSID, MAC-Filterung, Industriestandard: WEP, WPA, WPA2
Kompatibilität	802.11a	802.11b	802.11b, 802.11g	802.11b, 802.11g, 802.11n (teilweise 802.11a)	802.11a, 802.11b, 802.11g, 802.11n
Kommunikationsmodus	Ad-hoc oder Infrastruktur	Ad-hoc oder Infrastruktur	Ad-hoc oder Infrastruktur	Ad-hoc oder Infrastruktur	Ad-hoc oder Infrastruktur
Beschreibung	8 verfügbare Kanäle. Weniger störungsanfällig als 802.11b und 802.11g.	14 im 2,4-GHz-Band verfügbare Kanäle, davon 3 ohne Überlapp.	Bessere Sicherheitsfunktionen. 14 im 2,4-GHz-Band verfügbare Kanäle, davon 3 ohne Überlapp.	Wie 802.11g, nutzt aber zusätzlich das 5-GHz-Band, das auch von 802.11a verwendet wird. 802.11n kann mehrere Antennen verwenden, um Geschwindigkeit und Reichweite zu erhöhen.	Erweitert 802.11n um zusätzliche Streams und Bandreite und bietet im 5-GHz-Band höhere Geschwindigkeit. Nutzt MU-MIMO und Sendestrahlsteuerung zur Optimierung drahtloser Verbindungen.

Tabelle 20.1: Vergleich der 802.11-Standards

Tipp

Sehen Sie sich die Übungen zum Thema Funktechnologien im Abschnitt über Kapitel 20 unter `https://totalsem.com/100x` an, um Ihre Kenntnisse über die Unterschiede zwischen den 802.11-Standards zu vertiefen.

Tipp: 802.11ac-Geräte

Für die kommenden Generationen ist der Standard 802.11ac maßgeblich. Sie müssen die verschiedenen Varianten kennen. Besuchen Sie einen der großen Elektronikmärkte (oder recherchieren Sie online). Welche Varianten von 802.11ac-Geräten werden angeboten? Beachten Sie die Zahlen und Buchstaben, mit denen die Geräte gekennzeichnet sind. Bei den einfachsten (und preiswertesten) Modellen könnte die Bezeichnung beispielsweise AC1200 lauten. Ein Modell mit der Kennzeichnung AC1900 kann schon rund doppelt so teuer sein.

Letztlich unterscheiden sich die verschiedenen 802.11ac-Router und -WAPs vor allem durch die verwendete Frequenz, die Anzahl der Antennen und die Anzahl der verbauten Sende/Empfangsmodule. Die angegebenen Unterschiede der Geschwindigkeiten sind schon erstaunlich. Ein AC1200-Modul beispielsweise bietet im 5-GHz-Band einen Datendurchsatz von 867 Mbps, ein AC3100-Modul hingegen erreicht 2167 Mbps. In der Praxis sind die Unterschiede nicht so groß.

20.2.2 Andere drahtlose Standards

Wi-Fi dominiert den Markt drahtloser Netzwerke zwar eindeutig, ist aber nicht der einzige Standard. Viele kleine Netzwerke (soll heißen: zwei Geräte) verwenden Infrarot oder Bluetooth zur Kommunikation. mobile Geräte (Smartphones, Wearables oder einige Tablets) können sich per Mobilfunknetzwerk drahtlos verbinden. Häufig kommen auch weitere Standards zum Einsatz, um Smartphone oder Tablet mit der Stereoanlage im Auto, GPS-Empfängern, Fernsehgeräten, Flugdrohnen oder vielen anderen per Funk steuerbaren Geräten zu verbinden.

Drahtlose Infrarot-Netzwerke

Drahtlose Netzwerke auf Basis der Infrarot-Technologie werden heute meist übersehen, was möglicherweise an dem steigenden Interesse an neueren und schnelleren drahtlosen Standards liegt. Infrarot bietet aber immer noch eine sinnvolle Möglichkeit zur Dateiübertragung bei einigen älteren Geräten.

Bei der Kommunikation über Infrarot-Geräte wird das *IrDA*-Protokoll (*Infrared Data Association*) genutzt. Beim IrDA-Protokollstapel handelt es sich um einen weitverbreiteten Industriestandard, der von allen Windows-Versionen und praktisch der ganzen Branche unterstützt wird.

Hinweis

Apple- und Linux-Rechner unterstützen IrDA ebenfalls.

Geschwindigkeit und Reichweite von Infrarot-Netzwerken sind wenig beeindruckend. Infrarot-Geräte können Daten mit einer Geschwindigkeit von maximal 4 Mbps übertragen. Nicht allzu schlecht, aber auch nicht gerade rekordverdächtig. Die maximale Entfernung zwischen Infrarot-Geräten beträgt einen Meter. Für Infrarot-Verbindungen muss eine direkte Sichtverbindung bestehen und sie sind dadurch störanfällig. Alles, was den Lichtstrahl unterbricht, trennt auch die Infrarot-Verbindungen, sei es nun ein unbedacht platziertes Glas, ein Mitarbeiter, der zwischen Tischen hindurchgeht, oder auch nur helles Sonnenlicht, das den Infrarot-Transceiver trifft und für Störungen sorgt.

Infrarot wurde nur für die Herstellung von Punkt-zu-Punkt-Verbindungen zwischen zwei Geräten im Ad-hoc-Modus entwickelt. Einen Infrastruktur-Modus gibt es nicht. Sie können aber einen Infrarot-Zugriffspunkt (IR-AP) dazu verwenden, um über IrDA mit einem Ethernet-Netzwerk zu kommunizieren. Infrarot-Geräte arbeiten im Halbduplex-Betrieb, sodass ein Gerät immer nur entweder senden oder empfangen kann. Zwei Geräte können nicht gleichzeitig senden *und* empfangen. IrDA bietet zwar einen Modus an, der die Vollduplex-Kommunikation emuliert, dieser arbeitet aber eigentlich auch nur halbduplex. Im Hinblick auf die Sicherheit bietet das IrDA-Protokoll rein gar nichts, was Verschlüsselung oder Authentifizierung betrifft. Das Hauptsicherheitsmerkmal von Infrarot ist in der Tatsache zu sehen, dass Sie sich buchstäblich im Abstand einer Armeslänge befinden müssen, um eine

Verbindung herstellen zu können. Infrarot ist natürlich keine besonders gute Lösung für eine dauerhafte Netzwerkverbindung, eignet sich aber durchaus für die gelegentliche Übertragung von Dateien oder Druckaufträgen ohne viel Aufhebens.

In Tabelle 20.2 sind die wichtigsten Infrarot-Spezifikationen aufgeführt.

Max. Durchsatz	4 Mbps
Max. Reichweite	1 Meter
Sicherheit	Keine
Kompatibilität	IrDA
Kommunikationsmodus	Punkt-zu-Punkt, Ad-hoc

Tabelle 20.2: Infrarot-Spezifikationen

Bluetooth

Die drahtlose Bluetooth-Technologie (benannt nach dem im neunten Jahrhundert lebenden dänischen König Harald Blauzahn) wurde entwickelt, um Geräte innerhalb kleiner drahtloser »persönlicher Netzwerke« (*PAN – Personal Area Network*) für bestimmte Aufgabenstellungen untereinander zu verbinden. Einige Beispiele sind Headsets für Smartphones, PANs zur schnellen Verbindung zweier PCs zu einem Netzwerk und Eingabegeräten wie Tastatur und Maus. Bluetooth wurde *nicht* als umfassende Netzwerklösung konzipiert und soll auch nicht mit Wi-Fi konkurrieren.

Wie alle Technologien wurde auch Bluetooth über die Jahre hinweg mehrfach aktualisiert, um es schneller und sicherer zu machen. Die erste Generation (Versionen 1.1 und 1.2) unterstützt Geschwindigkeiten von etwa 1 Mbps. Die zweite Generation (2.0 und 2.1) ist mit der ersten abwärtskompatibel und unterstützt zusätzlich höhere Geschwindigkeiten über die sogenannte EDR (Enhanced Data Rate), die für Spitzengeschwindigkeiten von etwa 3 Mbps sorgt. Die dritte Generation (3.x + HS) erreicht bis zu 24 Mbps, wobei der Datentransport allerdings über eine 802.11-Verbindung erfolgt, die per Bluetooth ausgehandelt wird. Diese Funktionalität, die als +HS (High Speed) bezeichnet wird, ist optional. Anstatt ausschließlich auf weitere Geschwindigkeitserhöhungen zu setzen, konzentriert sich die vierte Generation (4.0, 4.1 und 4.2), die auch *Bluetooth Smart* genannt wird, auf die Verbesserung der Fähigkeiten zur Nutzung mit vernetzten »intelligenten« Geräten. Sie zeichnet sich durch niedrigeren Stromverbrauch, verbesserte Geschwindigkeit sowie erhöhte Sicherheit aus und bietet erstmals die Möglichkeit von IP-Verbindungen. Die fünfte Generation, die einfach nur *Bluetooth 5* heißt, bringt Optionen zur Erhöhung der Geschwindigkeit auf Kosten der Reichweite oder durch eine Änderung der Größe der Datenpakete mit. Bluetooth 5 bietet zudem eine bessere Unterstützung für IoT-Geräte (*Internet of Things*, Internet der Dinge), wie smarte Lautsprecher, Beleuchtungssysteme und so weiter.

Hinweis

In Kapitel 21 befasse ich mich ausführlich mit dem Internet der Dinge.

Die IEEE hat sich beim Standard 802.15 für drahtlose PANs an der ersten Bluetooth-Generation orientiert. Bluetooth verwendet eine Broadcast-Methode, bei der sehr schnell (rund 1.600 Mal pro Sekunde) zwischen den 79 im 2,45-GHz-Band verfügbaren Frequenzen gewechselt wird. Auf diese Weise ist Bluetooth kaum anfällig für Interferenzen.

Im Allgemeinen ist umso mehr Energie erforderlich, je weiter und schneller ein Gerät Daten sendet. Den Bluetooth-Entwicklern ist natürlich schon lange klar, dass bestimmte Geräte (wie z.B. Headsets) energiesparender arbeiten können, wenn sie Daten langsamer oder über geringere Entfernungen übertragen können. Aus diesem Grund gehören alle Bluetooth-Geräte einer von drei Kategorien an, die Obergrenzen für Stromverbrauch (in Milliwatt) und Reichweite festlegen (Tabelle 20.3).

Klasse	Max. Leistungsaufnahme	Max. Entfernung
Class 1	100 mW	100 Meter
Class 2	2,5 mW	10 Meter
Class 3	1 mW	1 Meter

Tabelle 20.3: Bluetooth-Klassen

Bluetooth ist dafür ausgelegt, den Kabelsalat zu beseitigen, der entsteht, wenn man verschiedene Peripheriegeräte (Tastatur, Maus, Drucker, Lautsprecher, Scanner usw.) mit dem PC verbindet. Es wird aber 802.11-basierte Netzwerkgeräte in absehbarer Zeit nicht ersetzen können. Dessen ungeachtet könnten die unlängst vorgestellten IP-Verbindungen dazu führen, dass zunehmend mehr Bluetooth-Datenverkehr auf 802.11-Geräten stattfindet.

Nachdem das geklärt ist, sind Geräte mit drahtlosen Bluetooth-Funktionen auf verschiedene Weise mit anderen drahtlosen Technologien vergleichbar:

- Wie Infrarot eignet sich auch Bluetooth für die einfache Dateiübertragung, wenn keine anderen verkabelten (oder schnelleren drahtlosen) Verbindungen verfügbar sind.
- Durch seine Geschwindigkeit und Reichweite eignet sich Bluetooth gut für drahtlose Druckerserver-Lösungen.

Die Bluetooth-Hardware wird entweder in viele der neueren mobilen elektronischen Kleingeräte wie Smartphones integriert oder als Adapter mit einem internen oder externen Erweiterungsbus verbunden. Bluetooth-Netzwerke werden über Ad-hoc-Verbindungen zwischen zwei Geräten oder über eine Art Infrastruktur-Modus und Bluetooth-Zugriffspunkte realisiert. Bluetooth-Zugriffspunkte ähneln stark den 802.11-basierten APs und verbinden drahtlose Bluetooth-PAN- und verkabelte LAN-Segmente.

Mobilfunknetze

Über Mobilfunknetze können sich Smartphones, Tablet-Computer oder andere mobile Geräte mit dem Internet verbinden. In den Lernzielen der CompTIA-Prüfung werden Mobilfunknetze zwar als allgemeiner Standard für drahtlose Netzwerke aufgeführt, für lokale Netzwerke werden sie aber eigentlich nicht verwendet. Viel gebräuchlicher ist es, sie für Verbindungen ins Internet zu nutzen. Eine in die Jahre gekommene Technologie verwendete Erweiterungskarten für den Zugriff auf das Internet, zu denen ich später kurz komme, falls eine Frage dazu in der Prüfung vorkommen sollte.

Hinweis

Mehr über Mobilfunknetze erfahren Sie in Kapitel 21, *Das Internet*.

1002

20.3 Installation und Konfiguration drahtloser Netzwerke

Die Einrichtung eines drahtlosen Netzwerks unterscheidet sich kaum von einem kabelgebundenen Netzwerk. Auch die physische Installation eines drahtlosen Netzwerkadapters ähnelt der eines kabelgestützten Netzwerkadapters. Bei beiden kann es sich um interne Steckkarten, PC-Cards oder externe USB-Geräte handeln. Sie installieren die Komponente einfach und überlassen PnP die Erkennung und die Ressourcenzuordnung. Wenn Sie dazu aufgefordert werden, dann installieren Sie die mit dem Gerät gelieferten Treiber und sind damit praktisch fertig.

Drahtlose Netzwerke sollten so konfiguriert werden, dass nur bestimmte drahtlose Knoten ein drahtloses Netzwerk benutzen können. Damit ist gleichzeitig für die Sicherheit der per Funk übertragenen Daten gesorgt.

20.3.1 WLAN-Konfiguration

WLAN-Netzwerke unterstützen sowohl den Ad-hoc- als auch den Infrastruktur-Modus. Welcher Modus verwendet wird, hängt davon ab, wie viele drahtlose Knoten unterstützt werden sollen, wie die Daten gemeinsam genutzt werden sollen und welche Verwaltungsanforderungen ansonsten gelten.

Ad-hoc-Modus

Drahtlose Ad-hoc-Netzwerke benötigen keinen WAP. Bei drahtlosen Netzwerken im *Ad-hoc-Modus* müssen nur die einzelnen drahtlosen Knoten mit demselben Netzwerknamen (SSID) konfiguriert werden und die IP-Adressen der Knoten müssen eindeutig sein. Abbildung 20.11 zeigt das EIGENSCHAFTEN-Dialogfeld eines drahtlosen Netzwerkadapters, in dem der Ad-hoc-Modus aktiviert werden kann.

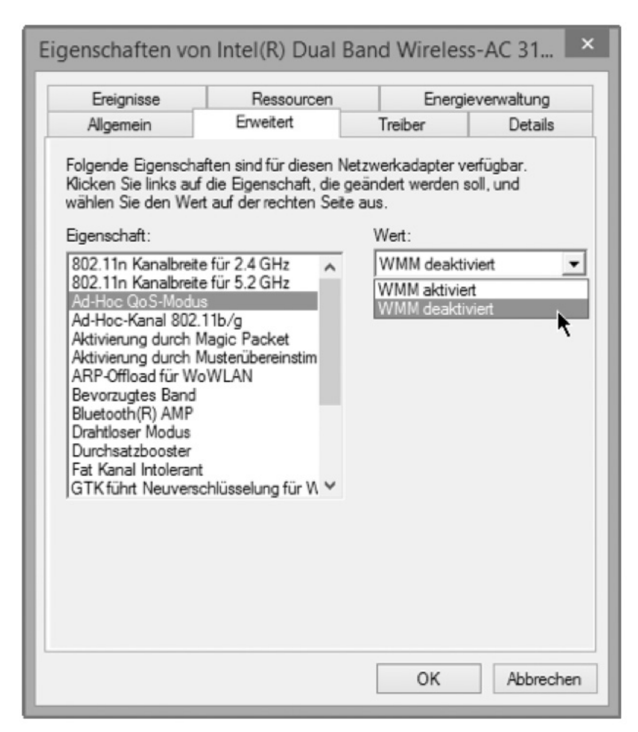


Abb. 20.11: Auswahl des Ad-Hoc-Modus im Dialogfeld EIGENSCHAFTEN eines WLAN-Adapters

Darüber hinaus müssen Sie normalerweise nur noch dafür sorgen, dass die Knoten unterschiedliche IP-Adressen verwenden, wobei auch dieser Schritt entfällt, wenn alle Knoten DHCP verwenden, und dass der Dienst für die Datei- und Druckerfreigabe auf allen Knoten ausgeführt wird.

Infrastruktur-Modus

Typischerweise sind im *Infrastruktur-Modus* ein oder mehrere WAPs mit einem kabelgebundenen Netzwerksegment (wie einem Unternehmensnetzwerk) oder dem Internet verbunden. Wie beim Ad-hoc-Modus müssen auch im Infrastruktur-Modus alle Knoten und WAPs des Netzwerks mit demselben

Netzwerknamen (SSID) konfiguriert werden. Abbildung 20.12 zeigt eine ältere Version von Ubuntus Dialogfeld zur Konfiguration eines WLAN-Adapters, in dem der Infrastruktur-Modus eingestellt ist.

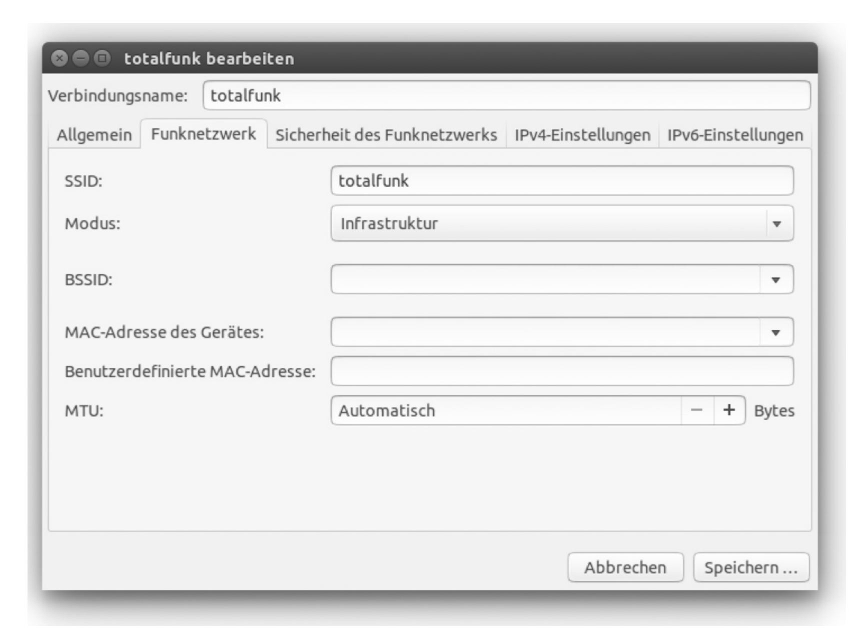


Abb. 20.12: Auswahl des Infrastruktur-Modus in den Einstellungen des Funknetzwerks

WAPs verfügen über einen integrierten Webserver und werden über ein Browser-gestütztes Einrichtungsprogramm konfiguriert. Typischerweise starten Sie auf einer der Client-Arbeitsstationen im Netzwerk den Webbrowser und geben die (vorkonfigurierte) IP-Adresse des WAPs ein (z.B. 192.168.1.1), um die Konfigurationsseite anzeigen zu lassen. Sie müssen dann Anmeldedaten eingeben, die Sie der WAP-Dokumentation entnehmen können (Abbildung 20.13). Diese sollten Sie bei der Ersteinrichtung möglichst sofort ändern. Die Konfigurationsprogramme unterscheiden sich naturgemäß bei den verschiedenen Herstellern und WAP-Modellen. Abbildung 20.14 zeigt den Hauptbildschirm für einen WLAN-Router der Firma Linksys. Um die Konfiguration zu erleichtern, liegt vielen WAPs ein webgestütztes Hilfsprogramm bei, das den WAP automatisch erkennt und den Benutzer schrittweise durch die Einrichtung führt.

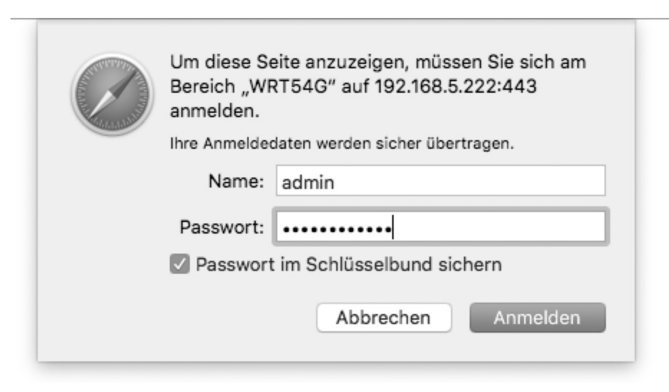


Abb. 20.13: Kennwortabfrage für einen WLAN-Router von Linksys

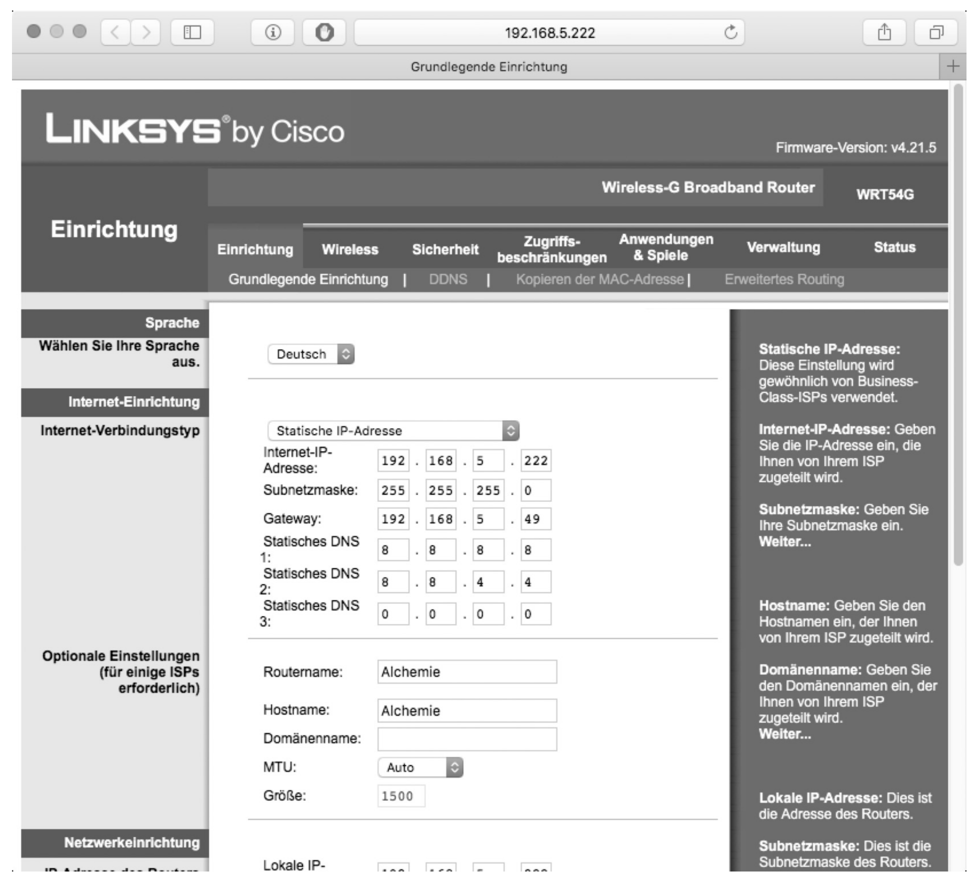


Abb. 20.14: Startbildschirm der Konfigurationsschnittstelle des Routers

Wenn Sie einen neuen WAP gekauft haben, stehen die Chancen nicht schlecht, dass der Hersteller bereits eine aktualisierte Firmware veröffentlicht hat. Das ist sogar noch wahrscheinlicher, wenn Sie den WAP schon länger besitzen. Bevor Sie den Router einrichten, damit die Benutzer darauf zugreifen können, sollten Sie überprüfen, ob neuere Firmware vorhanden ist und diese gegebenenfalls aktualisieren. Wie das genau funktioniert, erfahren Sie im Abschnitt über Problembehebung.

Konfigurieren Sie die SSID-Option an der entsprechenden Stelle. Denken Sie daran, dass es immer sicherer ist, wenn Sie selbst eine eindeutige SSID konfigurieren und nicht die wohlbekannte Vorgabe übernehmen, die einem Angreifer Hinweise auf Ihre Hardware geben könnte, der dann möglicherweise bekannte Schwachstellen des Geräts ausnutzt. Verwenden Sie keinen Namen, der Adresse, Standort oder andere Beschreibungen enthält, die es dem Angreifer ermöglichen könnten, das Gerät zu lokalisieren.

Die Kanalauswahl erfolgt zwar normalerweise automatisch, Sie können diese Option aber auch umkonfigurieren, wenn in einem Unternehmen bestimmte Anforderungen gelten (z.B. mehrere drahtlose Netzwerke in einem gemeinsamen Bereich). Mit WLAN-Detektoren kann man feststellen, auf welchem der Kanäle am wenigsten Datenverkehr stattfindet. Wenn Sie einen solchen Kanal auswählen, vermeiden Sie dadurch Probleme durch Interferenzen mit anderen WAPs. Die Clients überprüfen auf der Suche nach einer SSID automatisch alle Kanäle.

Um die Sicherheit weiter zu steigern, können Sie MAC-Filter benutzen. Abbildung 20.15 zeigt den Konfigurationsbildschirm für die MAC-Filterung bei einem Linksys-WAP. Geben Sie einfach die

MAC-Adressen der drahtlosen Knoten ein, denen der Zugang zum drahtlosen Netzwerk gestattet (oder verwehrt) sein soll. Aktivieren Sie die Verschlüsselung beim WAP und richten Sie einen eindeutigen Sicherheitsschlüssel ein. Konfigurieren Sie dann alle an das Netzwerk angeschlossenen drahtlosen Knoten mit demselben Sicherheitsschlüssel. Abbildung 20.16 zeigt das Dialogfeld für die Konfiguration des WAP2-Schlüssels bei einem Linksys-WAP.

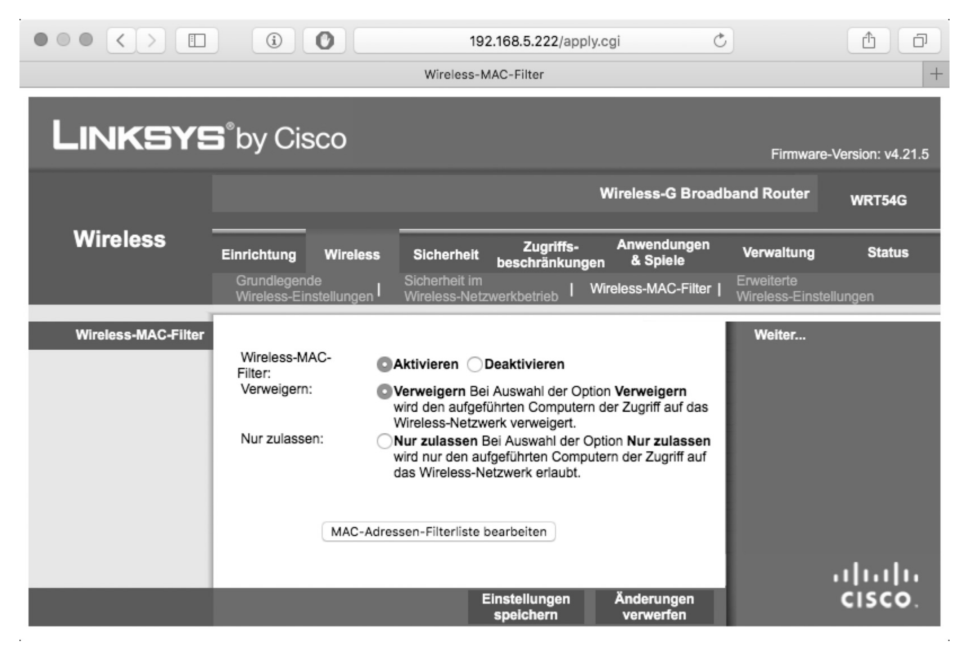


Abb. 20.15: Konfiguration der MAC-Filter

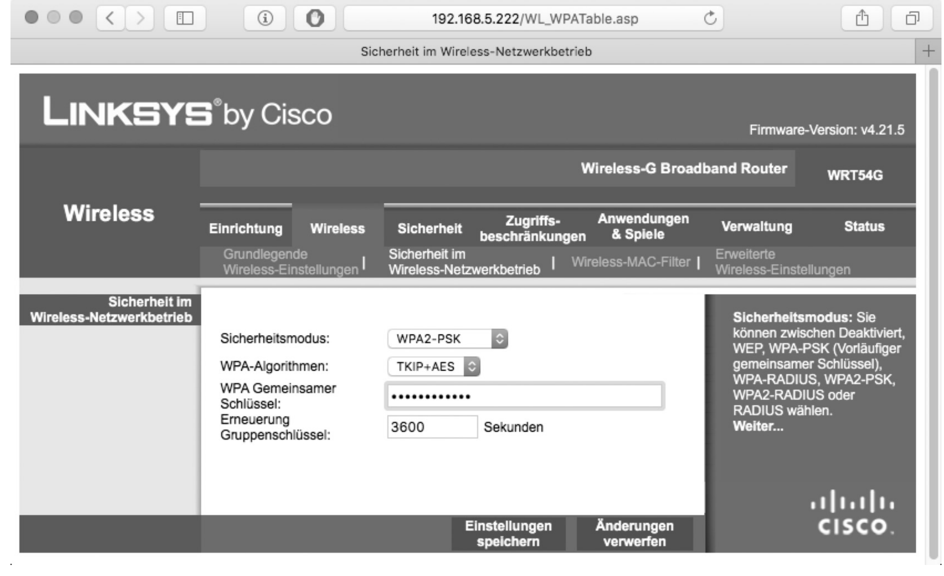


Abb. 20.16: Sicherheitseinstellungen

Wichtig

Wie bereits erwähnt, bietet das WEP-Protokoll zwar eine gewisse Sicherheit, kann aber relativ einfach geknackt werden. Verwenden Sie am besten WPA3 oder WPA2 oder zumindest WPA, bis Sie ein Upgrade vornehmen können.

Wenn Sie es mit älteren Geräten zu tun haben und gezwungen sind, WEP einzurichten, können Sie eine Reihe von Schlüsseln automatisch erzeugen lassen oder diese manuell vergeben. Sparen Sie sich die Denkarbeit und nutzen Sie das automatische Verfahren. Wählen Sie nun eine Verschlüsselungsebene. Hier haben Sie meist die Auswahl zwischen 64 und 128 Bit. Geben Sie dann ein eindeutiges Schlüsselwort (Passphrase) ein und klicken Sie die Schaltfläche ERSTELLEN an (bzw. die entsprechende Schaltfläche oder Option bei Ihrem WAP). Wählen Sie dann einen Vorgabeschlüssel aus und speichern Sie die Einstellungen. Die Verschlüsselungsebene, der Schlüssel und das Schlüsselwort müssen beim drahtlosen Client-Knoten genau den hier vorgenommenen Einstellungen entsprechen, ansonsten kommt keine Verbindung zustande. Bei vielen WAPs können Sie den Schlüssel auf einen Datenträger kopieren, um ihn bei den Client-Arbeitsstationen einfach importieren zu können. Ansonsten müssen Sie die Verschlüsselung manuell konfigurieren.

Die WPA- und WPA2-Verschlüsselung werden auf ähnliche Weise konfiguriert. Es gibt zwei Alternativen bei der Einrichtung von WPA/WPA2: *Personal/PSK* (*Pre-shared Key*) oder *Enterprise*. Bei WPA/WPA2-PSK (WPA/WPA2-Personal) handelt es sich um die in kleinen und Heimnetzwerken gängigste Variante (Abbildung 20.17). WPA/WPA2-Enterprise ist viel komplexer und erfordert zusätzliche Hardware (einen RADIUS-Server) und wird vorwiegend nur in wirklich professionellen drahtlosen Netzwerken mit hohen Sicherheitsanforderungen eingesetzt. Nach Auswahl dieser Option gibt es in manchen Fällen eine Unterauswahl, wie z.B. gemischten Betrieb, der es gestattet, dass ein WAP mit WPA2-Verschlüsselung auch WPA unterstützt. Für diese Einstellung sind die Bezeichnungen *PSK*, *Pre-Shared Key* oder nur *Personal* gebräuchlich.

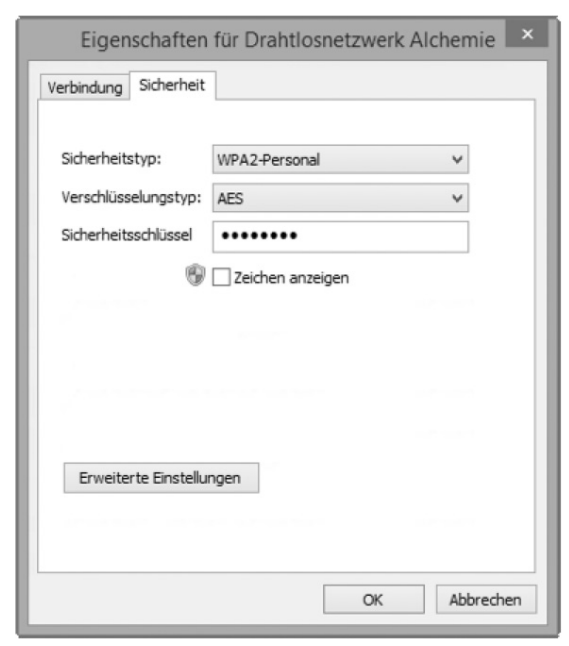


Abb. 20.17: Die Registerkarte mit den Einstellungen für die Verschlüsselung eines WLAN-Adapters

Sie sollten für den WAP und die NICs in Ihrem Netzwerk möglichst die WPA2-Verschlüsselung verwenden. Sie konfigurieren WPA2 auf dieselbe Weise wie WPA. Beachten Sie, dass Sie bei WPA2-Enterprise für die Authentifizierung einen sogenannten RADIUS-Server verwenden müssen (Abbildung 20.18). Größere Unternehmen sind tendenziell auf größere Sicherheit angewiesen, als ein einzelnes netzwerkweites Kennwort bieten kann. Deshalb müssen sich die Benutzer jeweils mit ihren eigenen Anmeldedaten einloggen.

Wichtig

Die Verwendung von Benutzername und Kennwort wird als *Ein-Faktor-Authentifizierung* bezeichnet, weil das beides Dinge sind, die Sie *wissen*. Für eine Mehrfaktor-Authentifizierung können zudem Dinge erforderlich sein, die Sie *besitzen* (wie einen Sicherheitsausweis) oder die ein biometrisches Merkmal darstellen (wie einen Fingerabdruck). In Kapitel 25 sehen wir uns genauer an, welche Rolle diese Faktoren bei der Authentifizierung spielen.

Zu diesem Zweck werden Authentifizierungsprotokolle wie RADIUS (*Remote Authentication Dial-In User Service*) oder TACACS+ (Terminal Acess Controller Acess-Control System Plus) eingesetzt. Dabei handelt es sich um Protokolle zur Authentifizierung von Benutzern, mit denen verwaltet wird, auf welche Ressourcen diese zugreifen dürfen. RADIUS ist teilweise verschlüsselt und verwendet UDP. TACACS+ ist vollständig verschlüsselt und nutzt TCP.

Wichtig

TACACS gibt es schon seit 1984. Es wurde weitgehend durch das abwärtskompatible TACACS+ ersetzt (das 1994 veröffentlicht wurde). In den Lernzielen ist lediglich von TACACS die Rede, aber ich hoffe doch, dass mögliche Fragen sich auf TACACS+ beziehen. Suchen Sie gegebenenfalls nach Hinweisen, falls es Fragen zum Thema TACACS gibt. Das ursprüngliche TACACS arbeitet unverschlüsselt, verwendet TCP oder UDP und erledigt nur die Authentifizierung. TACAS+ ist vollständig verschlüsselt, verwendet nur TCP und erledigt neben der Authentifizierung auch die Autorisierung, damit Benutzer auf bestimmte Ressourcen zugreifen können, was darüber hinaus protokolliert wird.

Auf diese Weise können Unternehmen nur Personen mit den richtigen Anmeldedaten die Verbindung mit ihren Wi-Fi-Netzwerken gestatten. Für ein Heimnetzwerk wählen Sie die PSK- bzw. Personal-Version von WPA3/WPA/WPA2. Entscheiden Sie sich für die beste verfügbare Verschlüsselung. Wenn WPA3 oder WPA2 angeboten wird, dann nutzen Sie es! Falls nicht, weichen Sie auf WPA aus. WEP wird auf sehr ähnliche Weise konfiguriert, ist aber eine wirklich schlechte Wahl für ein allgemein zugängliches Netzwerk. Wenn Sie Geräte, die nur WEP beherrschen, nicht aktualisieren oder ersetzen können, sollten Sie in Betracht ziehen, ein getrenntes Netzwerk dafür einzurichten.

Hinweis

Probieren Sie immer als Erstes WPA3- oder WPA2-Personal aus. Wenn es Clients gibt, die sich nicht mit dem WAP verbinden können, sollten Sie wenigstens WPA2- oder WPA-Personal nutzen. Konfigurieren Sie den gemischten Betrieb, damit neuere Rechner von der erhöhten Sicherheit profitieren können, die WPA3 oder WPA2 bieten.

Bei den meisten Heimnetzwerken können Sie für die Kanal- und Frequenzeinstellungen einfach die WAP-Voreinstellungen beibehalten. In einem Umfeld mit überlappenden Wi-Fi-Signalen müssen Sie diese aber oft anpassen. Die Option zur Einstellung des Wireless-Kanals finden Sie auf den WAP-Konfigurationsseiten. Abbildung 20.19 zeigt die Option zur Kanaleinstellung bei einem WAP der Firma Linksys.

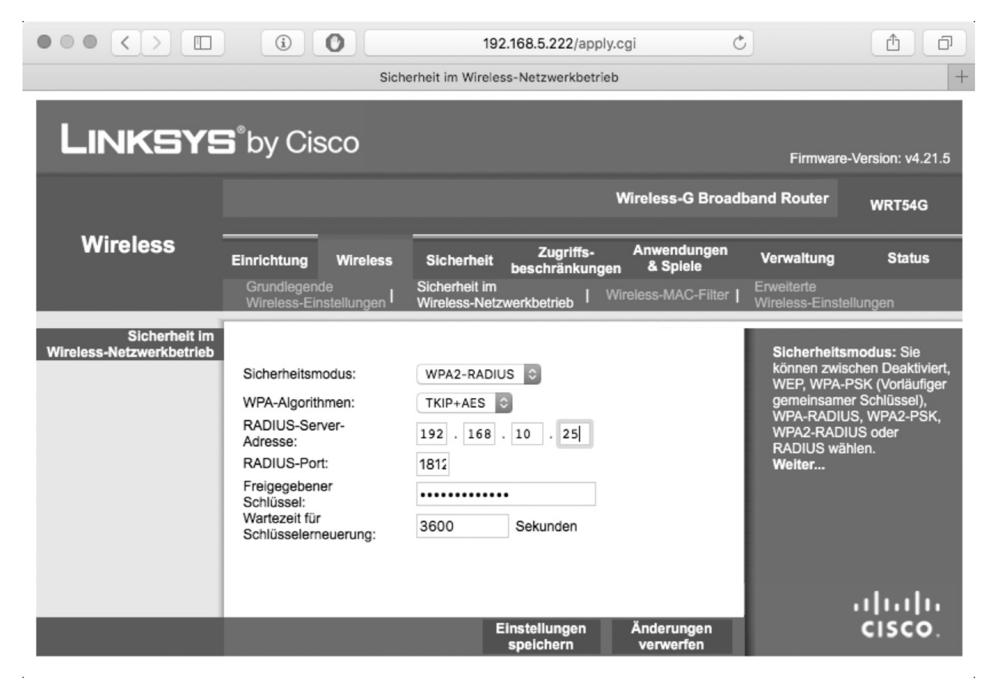


Abb. 20.18: Konfiguration eines RADIUS-Servers

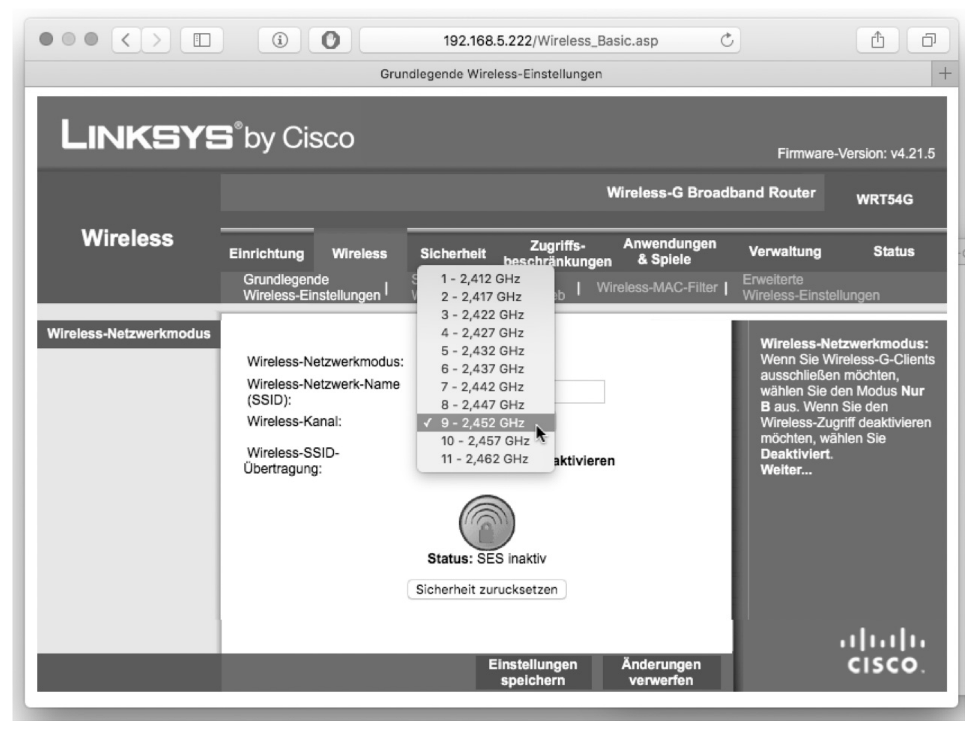


Abb. 20.19: Ändern des Kanals

Bei Dualband-WAPs (802.11n oder 802.11ac) können Sie wählen, welches Frequenzband (2,4 oder 5 GHz) für den Datenverkehr benutzt werden soll. In einem Umfeld mit überlappenden Signalen wird zumindest derzeit noch vorwiegend die 2,4-GHz-Frequenz genutzt. Neben anderen drahtlosen Geräten wie schnurlosen Telefonen verwenden auch Mikrowellen die 2,4-GHz-Frequenz und können für erhebliche Störungen sorgen. Sie können daher Konflikte mit Ihren Geräten vermeiden, wenn Sie stattdessen die 5-GHz-Frequenz benutzen. Abbildung 20.20 zeigt den Konfigurationsbildschirm für einen Dualband-802.11ac-WAP.



Abb. 20.20: Dualband-Konfiguration

Wichtig

Dieses Kapitel (und ein Großteil der Prüfung 1002) konzentriert sich auf drahtlose Netzwerke in SOHO-Umgebungen. Techniker nehmen die Konfiguration der WAPs anhand der integrierten Firmware der Geräte einzeln vor. Das ist auch schön und gut, falls es sich um Netzwerke handelt, in denen es nur eine Handvoll Zugriffspunkte gibt. Wenn es aber um eine ganze Universität oder ein großes Unternehmensgebäude geht, ist die Konfiguration unglaublich zeitraubend.

Vor einigen Jahren haben die Hersteller drahtlose LAN-Controller zur Zentralisierung der Konfiguration vieler Zugriffspunkte entwickelt. Ein Unternehmen kann Tausende Zugriffspunkte betreiben, die alle über eine einzelne Software-Schnittstelle konfiguriert werden. Diese Software kann auf einem lokalen Rechner ausgeführt werden, befindet sich aber heutzutage immer öfter in der Cloud. Das Ganze heißt dann *Cloud-basierter Netzwerk-Controller,* und solch ein Netzwerk könnte man *Cloud-verwaltetes WLAN* nennen.

Platzierung des Zugriffspunkts

Der optimale Ort für einen Zugriffspunkt hängt von dem abzudeckenden Bereich, die Ausstrahlung über dessen Grenzen hinweg und den Störungen durch andere (drahtlose) Geräte ab. Zunächst inspizieren Sie den Standort. Dazu können Sie einfach einen Laptop mit WLAN-Adapter starten und mit ihm nach bereits vorhandenen SSIDs suchen. Es kann sich dabei aber auch um eine komplexe Aufgabe handeln, für die Sie Dienstleister mit Spezialausrüstung beauftragen, die den Standort besichtigen und einen sorgfältigen Plan ausarbeiten sollen, in dem die besten Positionen für die WAPs und die zu verwendenden Wireless-Kanäle angegeben werden. Um dafür zu sorgen, dass das Wireless-Signal nur die gewünschten Orte erreicht und nicht unerwünscht abgelauscht werden kann, müssen Sie die richtige Antenne verwenden. Sehen wir uns deshalb an, welche Antennentypen erhältlich sind.

Omnidirektional und zentral Bei einem typischen Netzwerk sollen alle Bereiche abgedeckt werden, sodass man einen WAP mit einer omnidirektionalen Antenne zentral aufstellt (Abbildung 20.21). Bei einer omnidirektionalen Antenne werden die Funkwellen von dem WAP rundum ausgestrahlt. Der Vorteil besteht in der einfachen Nutzung, da alle Geräte, die sich im Signalradius befinden, potenziell auf das Netzwerk zugreifen können. Für die meisten drahtlosen Netzwerke und insbesondere im Heimbereich wird diese Kombination verwendet. Die übliche Antenne mit einem geraden Draht, die omnidirektional arbeitet, wird *Dipolantenne* genannt. Dipolantennen sind stabförmig, enthalten in ihrem Inneren jedoch zwei Antennen (oder Pole), die entlang der Achse des Stabs ausgerichtet sind – daher die Bezeichnung *Dipol.*

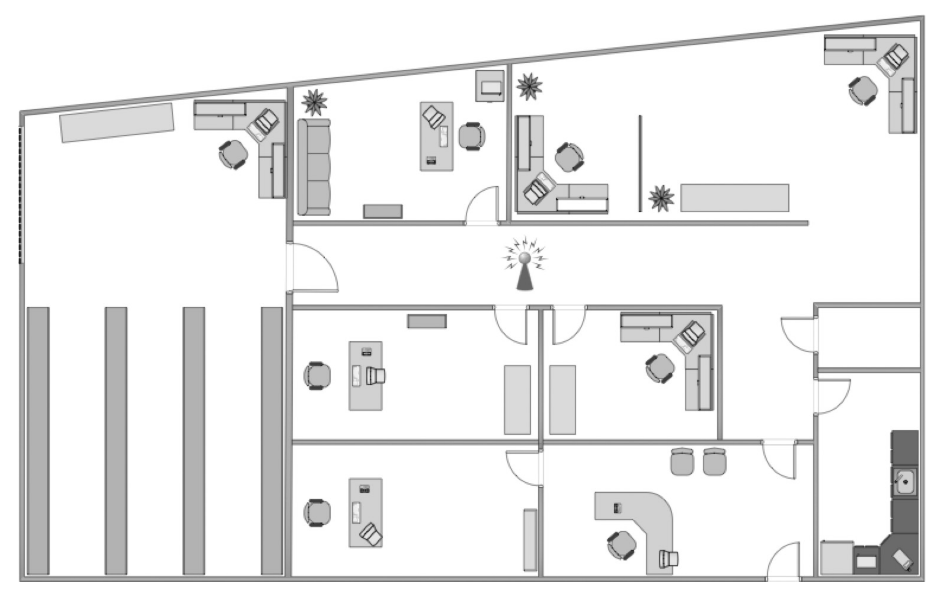


Abb. 20.21: Grundriss einer Wohnung mit zentralem WAP

Höhere Signalstärke Eine Antenne verstärkt und fokussiert die von einem WAP abgestrahlte Funkfrequenz (*RF – Radio Frequency*). Das *Verstärkungsverhältnis* (*Gain*) wird in Dezibel (dB) angegeben. Das Verstärkungsverhältnis eines typischen Zugriffspunkts liegt bei 2 dB, was ausreicht, um einen sinnvollen Bereich abzudecken, aber für einen sehr großen Raum bereits zu wenig ist. Um das Signal zu verstärken, wird eine leistungsfähigere Antenne benötigt. Bei vielen WAPs lassen sich die Antennen austauschen oder durch zusätzlich angeschlossene ersetzen. Um das Signal in einem Umfeld mit omnidirektionaler und zentral aufgestellter Antenne zu verstärken, ersetzen Sie einfach die ursprüngliche Antenne durch eine leistungsstärkere (Abbildung 20.22). Mit einer entsprechenden Antenne kann eine Verstärkung von bis zu 11 dB erreicht werden.



Abb. 20.22: Austauschantenne an einem WAP

Solche Antennen gibt es in vielen Varianten; sie verstärken schwache empfangene oder zu sendende Signale. Ein größerer Dipol bewirkt, dass Signale aus allen Richtungen besser empfangen werden können. Schüsselartige Parabolantennen und sogenannte Yagi-Antennen mit mehreren Elementen sind Richtantennen, die den Empfang lediglich in einer bestimmten Richtung verbessern. Wenn Sie eine Yagi-Antenne in Händen halten, wird sie Ihnen bekannt vorkommen, denn sie sehen aus wie die Hausantennen, die früher zum Empfang von Fernsehprogrammen verwendet wurden, sind allerdings sehr viel kleiner. Im Allgemeinen lässt sich sagen, dass eine Yagi-Antenne umso besser verstärkt, je mehr Elemente sie besitzt.

Eine Frage der Polarisation Antennen und die von ihnen übertragenen Signale weisen eine elektromagnetische Eigenschaft auf, die als *Polarisation* bezeichnet wird. Stark vereinfacht können Sie sich die Polarisation so vorstellen, dass die Signale die gleiche Ausrichtung wie die Antenne besitzen. Wenn die Antenne Ihres WAPs oder Ihres Computers nach unten oder oben weist, sind die übertragenen Signale vertikal polarisiert. Wenn Sie die Antenne hingegen auf die Seite legen, sind die Signale horizontal polarisiert. Natürlich kann die Antenne auch irgendwo zwischen horizontaler und vertikaler Ausrichtung positioniert werden. Vielleicht haben Sie sich noch keine Gedanken darüber gemacht, aber Ihr Laptop verwendet für gewöhnlich eine vertikale Polarisation, denn die Antenne verläuft auf der linken oder rechten Seite parallel zum Bildschirmrand. Und wenn der Laptop aufgeklappt ist, befindet sich der Bildschirm im Allgemeinen in einer mehr oder weniger senkrecht ausgerichteten Position.

Wichtig

Wenn Sie Verbindungen mit Clients unterstützen müssen, deren Antennen sowohl mit horizontaler als auch mit vertikaler Polarisation arbeiten, stellt es einen guten Kompromiss dar, die Antenne des WAPs in einem Winkel von 45 Grad auszurichten.

Um die bestmögliche Verbindung zwischen Client und WAP zu erzielen, sollten die Signale die gleiche Polarisation besitzen. Am schwächsten sind die zwischen WAP und Client übertragenen Signale, wenn eines der Geräte horizontal polarisierte Signale nutzt und das andere vertikal polarisierte. Bei Desktop-Computern ist es ziemlich einfach, dafür zu sorgen, dass die Antennen korrekt ausgerichtet sind. Bei Laptops Tablets und Smartphones hingegen ist es schon schwieriger, die richtige Antennenausrichtung zu gewährleisten. Falls Ihr WAP mehr als eine Antenne besitzt, sollten Sie diese unterschiedlich ausrichten, um den verschiedenen Clients Rechnung zu tragen. Aber welche Ausrichtungen sind die richtigen? Das lässt sich am einfachsten durch Testen herausfinden: Richten Sie eine der Antennen horizontal und die andere vertikal aus, und überprüfen Sie die Signalstärke an verschiedenen Orten des abzudeckenden Bereichs. Probieren Sie dann andere Ausrichtungen aus, bis Sie die höchste Signalstärke erzielen.

Hinweis

Wenn Sie in Erfahrung bringen möchten, ob es in einem Café, einer Bibliothek, am Flughafen usw. einen WLAN-Zugriffspunkt gibt (»Hotspot«), können Sie einen WLAN-Detektor verwenden. Diese Geräte sind etwa so groß wie eine Streichholzschachtel und verfügen über eine Anzeige, die darauf hinweist, wenn Sie sich in Reichweite eines WLAN-Netzwerks aufhalten. Es gibt auch Apps, die Ähnliches leisten und auf WLAN-fähigen Smartphones installiert werden können.

20.3.2 Bluetooth-Konfiguration

Wie alle anderen drahtlosen Netzwerklösungen unterstützen auch Bluetooth-Geräte PnP. Sie schließen einfach nur den Adapter an und folgen den Anweisungen zur Installation der verschiedenen Treiber und Konfigurationsprogramme (wenn Ihr Betriebssystem diese benötigt). Nach der Installation müssen Sie Bluetooth-Geräte miteinander koppeln (*Pairing*), um eine sichere Verbindung herzustellen, denn Sie möchten sicherlich nicht, dass sämtliche in Reichweite befindlichen Geräte sich automatisch

mit Ihrem Smartphone verbinden! Abbildung 20.23 zeigt den Bildschirm eines iPhones, das eine Anfrage zum Koppeln mit einem Mac namens »i5-2500MHz« erhält.

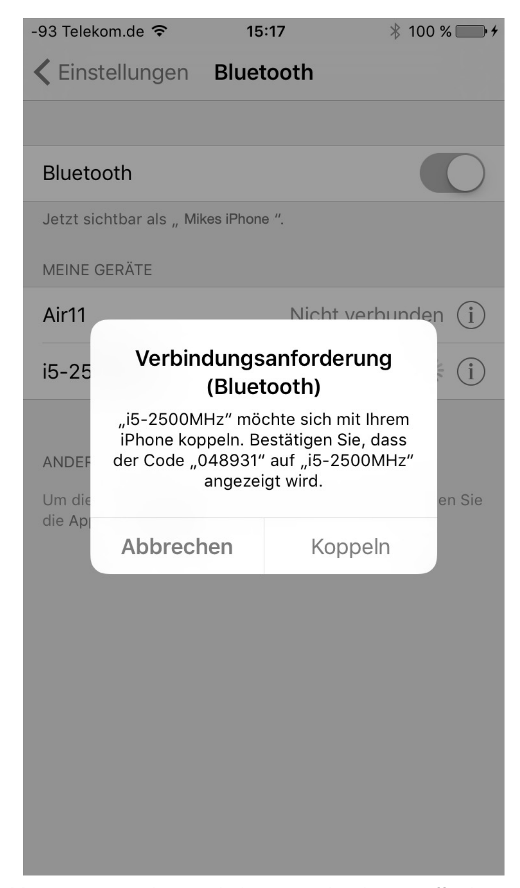


Abb. 20.23: Ein iPhone erhält eine Verbindungsaufforderung.

Zum Koppeln sind einige wenige Schritte nötig. Zunächst einmal muss natürlich Bluetooth aktiviert sein. Bei manchen Geräten, wie etwa Headsets, ist Bluetooth dauerhaft aktiviert, weil sie anders überhaupt nicht kommunizieren können. Auf Ihrem Computer hingegen können Sie Bluetooth im NETZWERK- UND FREIGABECENTER aktivieren oder deaktivieren.

Nach der Aktivierung müssen die Geräte in den Kopplungsmodus versetzt werden. Manche Geräte, wie etwa die Stereoanlage in meinem Auto, horchen permanent nach Kopplungsanfragen, andere müssen erst in einen entsprechenden Modus versetzt werden. Sind beide Geräte im Kopplungsmodus, entdecken sie einander und handeln automatisch Bluetooth-Version, Geschwindigkeit und weitere Merkmale der Verbindung aus.

Der letzte Schritt bei der Kopplung betrifft die Sicherheit. Dabei müssen Sie bestätigen, dass Sie die beiden Geräte tatsächlich miteinander koppeln möchten. Je nach Bluetooth-Version und Fähigkeiten der Geräte gibt es dafür verschiedene Verfahren. Manche Geräte bestätigen die Verbindung ohne weitere Benutzereingabe, bei anderen ist es erforderlich auf einem der Geräte (oder sogar auf beiden) einen kurzen Code einzugeben. Wenn Codes verwendet werden, sind diese meist vier oder sechs Zeichen lang, bei älteren Geräten vielleicht auch weniger. In der Dokumentation Ihres Geräts ist beschrieben, wie der Kopplungsvorgang im Detail abläuft.

Fertig, oder? Nun ja, fast. Eines bleibt noch zu tun: Überprüfen Sie, ob alles funktioniert. Gibt der Lautsprecher oder das Headset Töne von sich? Funktioniert das Bluetooth-Mikrofon, wenn Sie mit dem Smartphone Anrufe tätigen oder Sprachaufzeichnungen machen? Können Sie Musik von Ihrem Smartphone mit der Stereoanlage im Auto wiedergeben? Sie verstehen schon, was gemeint ist. Wenn irgendetwas nicht funktioniert, sollten Sie überprüfen, ob eins der beiden häufigsten Probleme vorliegt: gescheiterte/unvollständige Kopplung oder Fehlkonfiguration.

Die Kopplung geht schnell und kann leicht wiederholt werden. Eventuell müssen Sie die Kopplung auf einem der Geräte wieder entfernen. Versuchen Sie es nach der Entkopplung erneut. Sollte der Kopplungsvorgang gar nicht erst starten, funktioniert womöglich die Bluetooth-Verbindung überhaupt nicht. Vergewissern Sie sich, dass auf beiden Geräten Bluetooth aktiviert ist, sowie dass beide Geräte eingeschaltet und im Kopplungsmodus sind. Überprüfen Sie auch den Ladungszustand der Batterien (falls vorhanden) und die konfigurierten Einstellungen des Geräts.

Falls die Kopplung offenbar klappt, die Verbindung jedoch nicht funktioniert, liegt vermutlich eine Fehlkonfiguration vor. Prüfen Sie bei Audiogeräten, ob die Einstellungen für Mikrofoneingang und Lautsprecher korrekt sind. Verwenden Sie die gegebenenfalls vom Hersteller bereitgestellten Werkzeuge zur Fehlerdiagnose. Probieren Sie es so lange aus, bis es funktioniert oder bis Sie mit Sicherheit sagen können, dass die beiden Geräte nicht miteinander kompatibel sind oder dass ein Defekt vorliegt.

Um sich mit einem Bluetooth-PAN zu verbinden, ist ein wenig mehr Aufwand erforderlich als bei der Kopplung zweier Geräte. In den meisten Fällen wird solch eine Verbindung vom Betriebssystem gehandhabt. Abbildung 20.24 zeigt die Systemeinstellung NETZWERK in macOS mit einem verbindungsbereiten iPhone.

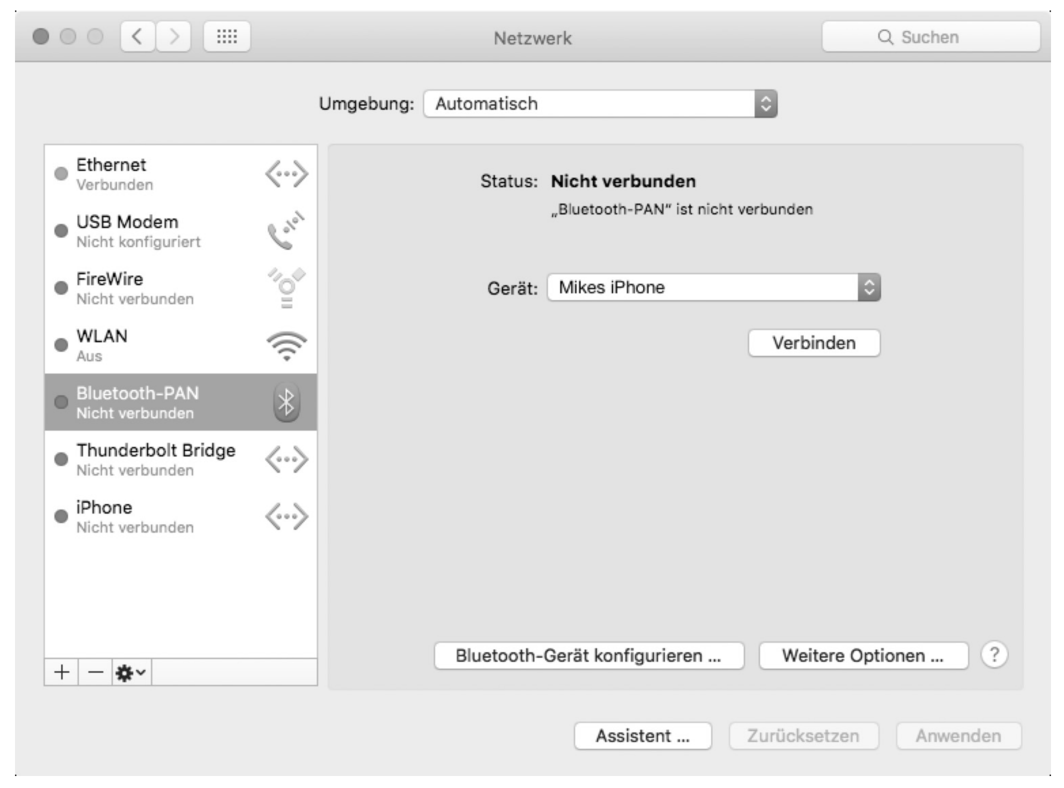


Abb. 20.24: macOS ist bereit, sich mit dem Bluetooth-PAN von »Mikes iPhone« zu verbinden.

Hinweis

Bluetooth-Zugriffspunkten zu Netzwerken werden Sie in der Praxis kaum begegnen. Moderne mobile Geräte wie Tablets oder Smartphones stellen ihre Internetverbindungen so gut wie immer über WLAN oder Mobilfunknetze her.

20.3.3 Konfiguration von Mobilfunkgeräten

Als der Zugriff auf Netzwerke, insbesondere auf das Internet, über Mobilfunknetze eingeführt wurde, entwickelten die Hersteller entsprechende Erweiterungskarten, um Computern – vor allem tragbaren Geräten – den Zugriff auf das Web unterwegs zu ermöglichen. Für die Konfiguration eines Mobilfunkadapters gab es keinen allgemeingültigen Standard, weil die Adapter und die Software bei den jeweiligen Herstellern, Anbietern und Netzbetreibern unterschiedlich aussahen. Die Mobilfunkanbieter machten die Installation der Adapter aber generell recht einfach.

Die meisten Adapter mussten Sie einfach nur anschließen, für gewöhnlich per USB, dann startete das Installationsprogramm automatisch. Treiber und andere Software befanden sich fast immer »an Bord« der Geräte selbst, sodass keine optischen Discs oder andere Installationsmedien nötig waren. Nach der Installation konnten Sie eine Anwendung starten, die eine Internetverbindung herstellte.

Es gibt schon eigenständige Mobilfunknetzkarten (und mit der Einführung von 5G-Netzwerken werden es vermutlich mehr werden). Heutzutage gebräuchlicher sind drahtlose Hotspots, wie in Abbildung 20.25. Die Geräte verbinden sich mit einem Mobilfunknetz (für den Zugriff müssen Sie natürlich bezahlen). Dann konfigurieren Sie Ihr Gerät so, dass es sich per WLAN mit dem Hotspot verbindet – schon haben Sie einen Internetzugang. In Kapitel 21 werde ich sehr viel ausführlicher auf WLAN-Hotspots und 5G eingehen.



Abb. 20.25: LTE-Hotspot von AT&T

20.4 Problembehebung bei drahtlosen Netzwerken

Drahtlose Netzwerke sind ein wahrer Segen, wenn sie korrekt funktionieren, können aber auch zu einem echten Ärgernis werden, wenn das nicht der Fall ist. Daher werde ich Ihnen nun einigen praktischen Ratschlägen geben, mit deren Hilfe Sie Probleme im Zusammenhang mit der Hardware, Software und der Konfiguration von drahtlosen Geräten leichter beheben können.

Wie in jeder Situation, in der eine Fehlerbehebung ansteht, müssen Sie auch hier die Aufgabe in logische Schritte unterteilen. Im ersten Schritt sollten Sie den Umfang des Problems mit dem drahtlosen Netzwerk in Erfahrung bringen. Fragen Sie sich selbst Folgendes:

- Wer ist vom Problem betroffen?
- Wie äußert sich das Netzwerkproblem?
- Wann ist das Problem erstmals aufgetreten?

Die Antworten auf diese Fragen bestimmen zumindest anfangs die Richtung Ihrer weiteren Nachforschungen.

Wer ist also betroffen? Wenn alle Geräte im Netzwerk (kabelgebundene und drahtlose) keine Verbindungen mehr herstellen können, dann ist das Problem weitreichender und betrifft nicht nur die drahtlosen Geräte. Die weitere Problembehebung sieht dann wie bei jedem Netzwerkausfall aus. Wenn Sie ermittelt haben, welche drahtlosen Knoten betroffen sind, lässt sich leichter feststellen, ob das Problem bei einem oder mehreren Wireless-Clients oder einem oder mehreren Zugriffspunkten liegt.

Wenn Sie die Anzahl der betroffenen Geräte eingegrenzt haben, müssen Sie im nächsten Schritt herausfinden, welchen spezifischen Fehler die Benutzer wahrnehmen. Wenn Sie zwar auf einige, aber nicht auf alle Netzwerkdienste zugreifen können, dann ist es unwahrscheinlich, dass sich das Problem auf ihre drahtlosen Geräte beschränkt. Ist beispielsweise zwar der Zugriff auf das Internet, nicht aber auf freigegebene Ressourcen auf einem Server möglich, dann handelt es sich wahrscheinlich um ein Problem im Zusammenhang mit Berechtigungen und nicht um ein Problem der drahtlosen Geräte.

Schließlich ermitteln Sie, wann das Problem erstmals aufgetreten ist. Was hat sich geändert und könnte den Verbindungsabbruch erklären? Hat jemand die WLAN-Konfiguration geändert? Wenn das Netzwerk z.B. noch vor zwei Minuten tadellos funktioniert hat, dann aber der WPA2-Schlüssel oder die Verschlüsselungsmethode des Zugriffspunkts geändert wurde und nun niemand mehr das Netzwerk sehen kann, dann haben Sie die Lösung oder zumindest Ihren Schuldigen gefunden! Gab es im Büro einen Stromausfall, Spannungsspitzen oder -schwankungen? Das könnten Gründe für einen WAP-Ausfall sein. Das führt uns zum nächsten Schritt der Strategie zur Fehlersuche, die Ich in Kapitel 1 erörtert habe.

Sobald Sie die Fragen nach dem Wer, Was und Wann geklärt haben, können Sie mit der eigentlichen Problembehebung beginnen. Typischerweise wird das Problem die Hardware, die Software, die Verbindungen oder die Konfiguration betreffen.

Hardwareprobleme

WLAN-Hardwarekomponenten im Netzwerk können wie alle anderen Hardwarekomponenten falsch bedient, behandelt oder installiert werden. Bei vermuteten Hardwareproblemen ist der Techniker in Ihnen gefragt.

Sehen Sie im Geräte-Manager von Windows nach, ob beim WLAN-Adapter Fehler oder Konflikte angezeigt werden. Wenn ein Ausrufezeichen neben dem Gerät angezeigt wird, dann handelt es sich um einen Treiberfehler. Ein nach unten weisender Pfeil neben dem Gerät bedeutet, dass es deaktiviert wurde. Installieren Sie den Gerätetreiber neu oder aktivieren Sie das Gerät wieder, falls möglich.

Wenn das Gerät im Geräte-Manager überhaupt nicht angezeigt wird, dann sitzt es möglicherweise nicht richtig in seinem Steckplatz oder eine PC Card bzw. ein USB-Adapter wurde nicht richtig oder nicht vollständig eingesteckt. Derartige Probleme lassen sich leicht beheben. Entfernen Sie das betroffene Gerät und installieren Sie es erneut.

Hinweis

Wie bei allen Rechnerproblemen sollten Sie auch hier nicht vergessen, den Rechner erst einmal neu zu starten, bevor Sie überhaupt Änderungen an der Konfiguration oder der Hardware vornehmen!

Softwareprobleme

Wenn Sie bereits geprüft haben, ob die richtigen Treiber für Ihre Hardware verwendet werden, nach welchen Softwareproblemen könnten Sie dann noch suchen? Dabei fallen einem sofort zwei Dinge ein: das WLAN-Konfigurationsprogramm und die WAP-Firmware-Version.

Wie ich bereits erwähnt habe, arbeiten manche WLAN-Geräte nur dann richtig, wenn man erst die Treiber des Herstellers und das Konfigurationsprogramm installiert, bevor man das Gerät anschließt. Das gilt insbesondere für USB-WLAN-Adapter. Wenn Sie anders vorgegangen sind, dann müssen Sie den Geräte-Manager starten, das Gerät dort deinstallieren und anschließend von vorn beginnen.

Wenn Sie Ihr neues Gerät auspacken, ist die darauf befindliche Firmware möglicherweise bereits veraltet. Das Problem äußert sich dann häufig so, dass die Clients zwar eine Verbindung herstellen können, die aber derart langsam ist, dass die Verbindung häufig abbricht. Vielleicht stellen Sie auch nach einer Woche fest, dass die Clients sich zwar mit dem WAP verbinden können, der Internetzugang aber erst wieder funktioniert, wenn Sie den WAP neu starten. Unter Umständen können sich Apple-Geräte nicht mit dem Zugriffspunkt verbinden oder ihnen wird nicht die angezeigte Geschwindigkeit bereitgestellt. Entscheidend ist hier, dass Sie nach merkwürdigem oder fehlerhaftem Verhalten Ausschau halten.

Die Hersteller veröffentlichen regelmäßig Firmware-Aktualisierungen, um Probleme wie diese und viele andere zu beheben. Es ist daher sinnvoll, die Firmware des Zugriffspunkts zu aktualisieren. Suchen Sie die Website des Herstellers auf und sehen Sie nach, ob eine aktuellere Firmware-Version verfügbar ist. Dazu benötigen Sie die genaue Modellbezeichnung, die Seriennummer und die derzeitige Firmware-Version Ihres Geräts. Das ist wirklich wichtig, da die Installation der falschen Firmware-Version Ihr Gerät garantiert unbrauchbar machen würde!

Aktuelle WAPs bringen oft eine Webschnittstelle für Administratoren mit, die es gestattet, die neu heruntergeladene Firmware einzuspielen. Manche davon können sie sogar selbst herunterladen und aktualisieren. Da es zu viele verschiedene WAPs gibt, um sie an dieser Stelle zu behandeln, sollten Sie auch hier den Anleitungen des Herstellers zur Aktualisierung der Firmware genauestens folgen.

Hinweis

Bei der Aktualisierung der Firmware beliebiger Geräte, auch Ihrem WAP, besteht immer die Möglichkeit, dass etwas schiefgeht und das Gerät dann unbrauchbar ist. Techniker sprechen dann gern von »Bricking« (engl. *brick* = Ziegelstein). Warum? Weil das Gerät zur Erledigung seiner Aufgabe dann ebenso nützlich wie ein Ziegelstein ist.

20.4.1 Verbindungsprobleme

Richtig konfigurierte WLAN-Clients sollten sich automatisch und schnell mit der gewünschten SSID verbinden, sofern Client und WAP dasselbe Frequenzband unterstützen. Wenn das nicht funktioniert, dann ist ein wenig Fehlersuche angesagt. Die meisten WLAN-Verbindungsprobleme lassen sich entweder auf eine falsche Konfiguration (z.B. ein falsches Kennwort) oder eine zu geringe Signalstärke zurückführen. Ist das Signal zu schwach, funktionieren selbst richtig konfigurierte WLAN-Clients nicht. WLAN-Clients benutzen ein Balkendiagramm (mit üblicherweise fünf Balken) zur ungefähren Anzeige der Signalstärke. Wird kein Balken angezeigt, wird auch kein Signal empfangen, während fünf Balken auf eine (nahezu) maximale Signalstärke hinweisen. Ein zu schwaches Signal kann zu langsamen Verbindungen und temporären Verbindungsausfällen führen.

Bei der Diagnose und Behebung von Problemen mit der Konfiguration oder der Signalstärke werden dieselben Verfahren wie bei kabelgebundenen Netzwerken verwendet. Werfen Sie zunächst einen Blick auf die Verbindungstatus-LED (Link) der WLAN-NIC, sofern vorhanden, um zu prüfen, ob Datenpakete vom und zum Netzwerk weitergeleitet werden. Dann benutzen Sie das Konfigurationsprogramm des WLAN-Adapters. In Abbildung 20.26 sehen Sie die Anzeige des Verbindungsstatus und der WLAN-Signalstärke in Windows 10.

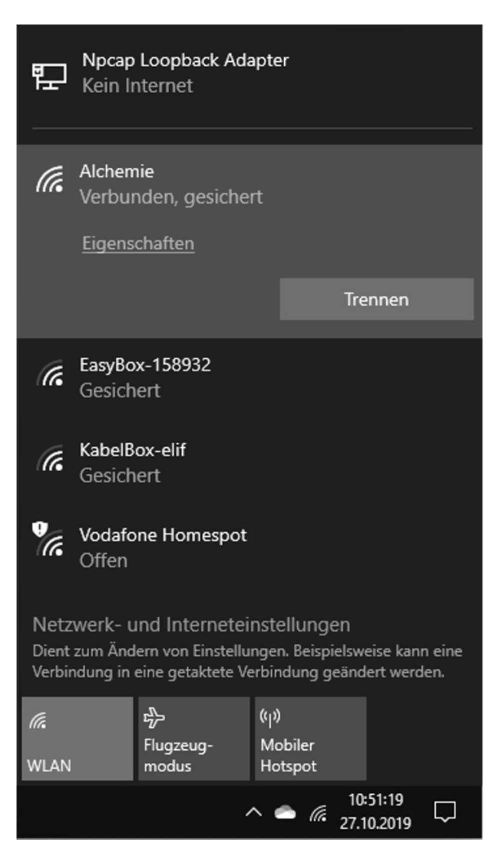


Abb. 20.26: Verbindungsstatus und Signalstärke in Windows 10

Der Verbindungsstatus gibt an, ob ein WLAN-Adapter mit einem drahtlosen Netzwerk verbunden ist oder nicht. Wenn beim Status angezeigt wird, dass der Rechner momentan keine Verbindung hergestellt hat, dann besteht möglicherweise ein Problem mit Ihrem WAP. Wenn das Signal zu schwach ist, um es empfangen zu können, dann befinden Sie sich eventuell außerhalb der Reichweite Ihres Zugriffspunkts oder ein anderes Gerät stört die Verbindung.

Diese Probleme lassen sich auf verschiedene Weise beheben. Da Funksignale von Objekten reflektiert werden, können Sie versuchen, ob sich die Signalstärke bei kleinen Änderungen der Antennenposition verbessert. Sie können die Standardantenne gegen eine mit größerer Signalverstärkung austauschen. Sie können den PC oder den Zugriffspunkt oder das die Störungen verursachende Gerät an einem anderen Ort aufstellen.

Andere drahtlose Geräte, die denselben Frequenzbereich wie Ihre drahtlosen Knoten benutzen, können ebenfalls Störungen verursachen. Schnurlose Telefone, Funkklingeln usw. sind mögliche Störenfriede. Möglicherweise können Sie die Störungen durch die anderen drahtlosen Geräte dadurch umgehen, dass Sie den von Ihrem Netzwerk benutzten Kanal ändern. Vielleicht können Sie auch die von dem störenden Gerät verwendete Funkfrequenz ändern. Wenn das nicht möglich ist, dann verschieben Sie das störende Gerät an einen anderen Ort oder ersetzen es durch ein anderes.

Konfigurationsprobleme

Bei allem nötigen Respekt vor all den guten Netzwerktechnikern da draußen: Die häufigste Fehlerursache bei WLAN-Problemen stellen falsch konfigurierte Hardware oder Software dar. Richtig, diese

gefürchteten *Benutzerfehler*! Angesichts der Komplexität drahtloser Netzwerke ist das aber gar nicht so überraschend. Letztlich muss nur ein Finger auf der Tastatur verrutschen, um die Konfiguration vollständig über den Haufen zu werfen. Zumeist treten die Fehler bei der SSID und der Sicherheitskonfiguration auf, allerdings haben Dualband-Router die Sache weiter verkompliziert.

Überprüfen Sie erst bei Ihrem Zugriffspunkt und dann bei den betroffenen drahtlosen Netzwerkknoten die SSID-Konfiguration (für alle in Gebrauch befindliche Bänder). Bei den meisten drahtlosen Geräten können Sie beliebige Zeichen und auch Leerzeichen in der SSID verwenden. Passen Sie auf, dass Sie keine Leerzeichen an Stellen einfügen, an denen sie nichts zu suchen haben, wie z.B. hinter allen anderen Zeichen im Feld mit dem Netzwerknamen.

Manchmal kommt es vor, dass Clients, die sich bislang immer problemlos mit einem WAP verbinden konnten, der eine bestimmte SSID besitzt, plötzlich keine Verbindung mehr aufnehmen können. Unter Umständen wird auf dem Client eine Fehlermeldung wie »SSID nicht gefunden« angezeigt, dem muss aber nicht so sein. Für dieses Verhalten gibt es mehrere mögliche Erklärungen und das Problem lässt sich meist leicht beheben. Die einfachste Ursache ist, dass der WAP gar nicht in Betrieb ist – das kann leicht festgestellt und behoben werden. Am anderen Ende des Spektrums möglicher Ursachen sind Konfigurationsänderungen am WAP. Wenn die SSID eines WAPs geändert oder die SSID-Annoncierung deaktiviert wird, kann der Client sich nicht mehr verbinden. Um den Fehler zu beheben, kann entweder die Änderung am WAP rückgängig gemacht werden oder Sie passen die Konfiguration des Clients an. Möglicherweise kann sich ein Client nicht mit einem neuen WAP verbinden, obwohl er dieselbe SSID und dieselben Einstellungen verwendet wie der alte. Löschen Sie in diesem Fall das Verbindungsprofil des Clients und erstellen Sie ein neues.

Wenn Sie MAC-Adressfilter nutzen, überzeugen Sie sich davon, dass sich die MAC-Adresse des Clients, der auf das Netzwerk zuzugreifen versucht, in der Liste der zulässigen Benutzer befindet. Darauf sollten Sie insbesondere achten, wenn Sie Adapter bei Rechnern austauschen oder neue Rechner zum WLAN hinzukommen.

Überprüfen Sie, ob die Sicherheitskonfigurationen auch wirklich bei allen drahtlosen Knoten und Zugriffspunkten übereinstimmen. Wird ein Schlüssel falsch eingegeben, kann der betroffene Knoten selbst bei optimaler Signalstärke nicht mit dem WLAN kommunizieren! Denken Sie daran, dass viele Zugriffspunkte Schlüssel auf Speichersticks oder Wechselmedien exportieren können. Dann lässt sich der Schlüssel leicht über das Konfigurationsprogramm des WLAN-Adapters auf einem PC importieren. Beachten Sie außerdem, dass die Verschlüsselungsverfahren bei den Zugriffspunkten und den WLAN-Knoten übereinstimmen müssen. Wenn Ihr WAP für die WPA2-Verschlüsselung konfiguriert ist, dann muss sie auch von allen Knoten benutzt werden.

20.5 Wiederholung

20.5.1 Fragen

1. Welcher der folgenden 802.11-Standards funktioniert nur im 5-GHz-Band?
   A. 802.11g
   B. 802.11n
   C. 802.11ac
   D. 802.11i
2. Welches Verschlüsselungsprotokoll bietet die beste Sicherheit?
   A. Hi-Encrypt
   B. WEP
   C. WPA
   D. WPA2

3. Mit welchem Gerät können Sie die Fähigkeiten eines drahtlosen Netzwerks erweitern?
   A. WAP
   B. WEP
   C. WPA
   D. WPA2
4. In welchem Modus werden alle WLAN-Geräte direkt miteinander verbunden?
   A. Ad-hoc-Modus
   B. Ring-Modus
   C. Infrastruktur-Modus
   D. Mesh-Modus
5. Was bestimmt den Namen eines drahtlosen Netzwerks?
   A. EAP
   B. MAC-Adresse
   C. SSID
   D. WAP
6. Durch welche Technologie können 802.11n-Netzwerke mehrere simultane Verbindungen herstellen und damit eine höhere Geschwindigkeit als die bisherigen WLAN-Standards erreichen?
   A. Nutzung der 2,4-GHz-Frequenz
   B. Nutzung der 5-GHz-Frequenz
   C. MIMO
   D. WPA2
7. Welche Spitzentransferraten lassen sich mit der IrDA-Technologie erreichen?
   A. 2 Mbps
   B. 4 Mbps
   C. 11 Mbps
   D. 54 Mbps
8. Welche Art Netzwerk steht Computern über die Bluetooth-Technologie zur Verfügung?
   A. BAN (Bluetooth Area Network)
   B. PAN (Personal Area Network)
   C. LAN (Local Area Network)
   D. WAN (Wide Area Network)
9. Wie nennt man die bei drahtlosen Zugriffspunkten übliche omnidirektionale Antenne?
   A. Bipolantenne
   B. Dipolantenne
   C. Omniantenne
   D. Funkantenne
10. Ralph hat in seinem Haus ein drahtloses Netzwerk installiert. Der drahtlose Zugriffspunkt befindet sich an zentraler Position in der Küche. Das WLAN funktioniert zwar im Wohnzimmer und im Esszimmer tadellos, aber so gut wie gar nicht im Schlafzimmer. Was ist vermutlich die Ursache?
    A. Interferenzen durch ein Objekt aus Metall
    B. Falsche Antenneneinrichtung
    C. Verwendung der Standard-SSID
    D. Die SSID ist mit der eines Nachbarn identisch

20.5.2 Antworten

1. **C.** Der Standard 802.11.ac funktioniert nur im 5-GHz-Band. 802.11g nutzt das 2,4-GHz-Band, 802.11n funktioniert in beiden und 802.11i beschreibt den Sicherheitsstandard, der besser unter der Bezeichnung WPA2 bekannt ist.
2. **D.** WPA2 ist die beste Verschlüsselung der hier aufgelisteten Technologien.
3. **A.** Mit einem drahtlosen Zugriffspunkt (WAP – Wireless Access Point) lassen sich die Fähigkeiten eines WLANs erweitern.
4. **A.** In Netzwerken im Ad-hoc-Modus verbinden sich alle Knoten direkt miteinander.
5. **C.** Bei der SSID handelt es sich um den Namen eines drahtlosen Netzwerks.
6. **C.** Mit der MIMO-Technologie (Multiple In/Multiple Out) lassen sich mehrere Antennen verwenden. Sie ermöglicht in 802.11n-Netzwerken wesentlich höhere Geschwindigkeiten als in den älteren WLANs.
7. **B.** Die Datentransferraten mit dem IrDA-Protokoll erreichen maximal 4 Mbps.
8. **B.** Bluetooth erzeugt PANs (Personal Area Networks).
9. **B.** Omnidirektionale Standardantennen werden Dipolantennen genannt.
10. **A.** Achten Sie auf Mikrowellengeräte, Kühlschränke und Rohrleitungen in den Wänden. Sie können WLAN-Funksignale stören und zu Funklöchern führen.

Das Internet 21

Themen in diesem Kapitel:

- Funktionsweise des Internets
- Internetverbindung einrichten
- Verwendung von Internet-Dienstprogrammen
- Fehlerbehebung bei Internetverbindungen

Stellen Sie sich einmal vor, dass Sie nach einem langen Arbeitstag voller Reparaturen an PCs nach Hause kommen, sich vor Ihren nagelneuen Computer setzen, das einzige auf dem Bildschirm in einer Ecke versteckte Symbol anklicken und sich plötzlich inmitten einer fantastischen Szenerie befinden, in der 100 m hohe Bäume sich an schneeweißen Sandstränden wiegen und Flugsaurier über den Himmel gleiten. Die ganze Zeit über sprechen Sie mit einem kleinen Gnom mit spitzen Ohren und langer Robe darüber, dass Sie auf der Suche nach einem Ungeheuer einen Berg besteigen wollen ... Ist das SciFi im Fernsehkanal? Oder Spielbergs neueste Inszenierung? Wie wäre es mit einem interaktiven Spiel, an dem Millionen von Menschen überall auf dem Planeten täglich per Internetverbindung teilnehmen? Mit der letzten Vermutung liegen Sie richtig!

Dieses Kapitel behandelt die Fertigkeiten, die Sie als PC-Techniker zur Unterstützung aller Kunden besitzen sollten, die eine Verbindung mit dem Internet herstellen wollen. Es beginnt mit einem kurzen Abschnitt darüber, wie das Internet funktioniert, und behandelt dabei auch die Konzepte der Konnektivität. Anschließend erfahren Sie mehr über die Hardware, die Protokolle und die Software, die das Internet nutzbar machen. Abschließend betrachten wir die Fehlerbehebung einer nicht funktionierenden Internetverbindung. Und los geht's!

Geschichte und Konzepte

21.1 Wie das Internet funktioniert

Das Internet bietet den Benutzern über riesige Entfernungen hinweg die Möglichkeit, miteinander zu kommunizieren, und dazu ist oftmals nur ein Wimpernschlag erforderlich. Als PC-Techniker müssen Sie wissen, wie PCs mit der Außenwelt kommunizieren, und zwar aus zwei Gründen: Als Erstes können Sie mit konkretem Hintergrundwissen über den Prozess und die Komponenten der Kommunikation effektiv Fehlerbehebung betreiben, wenn Probleme auftreten. Zweitens müssen Sie mit Netzwerkspezialisten fachmännisch kommunizieren können, wenn diese zur Lösung von schwierigeren Problemen gerufen werden.

21.1.1 Internet-Schichten

Ihnen ist zweifelsohne bekannt, dass das Internet aus Millionen von Computern besteht, die alle verknüpft sind und damit das größte Netzwerk auf der Erde bilden. Viele Leute wissen jedoch nicht viel darüber, wie diese Computer organisiert sind. Um alles reibungslos am Laufen zu halten, ist das Internet in Gruppen eingeteilt, sogenannte *Schichten* (*Tiers*). Die Hauptschicht, Tier 1, besteht aus einigen wenigen Unternehmen, den sogenannten Tier-1-Providern. Die Tier-1-Provider besitzen eigene *Backbones*: Hochgeschwindigkeits-Weitverkehrsnetze aus Glasfaser. Diese Backbones verknüpfen die größten Städte der Erde (nicht alle Tier-1-Backbones sind mit allen Städten verbunden) und treffen sich an speziellen Orten, sogenannten *NAPs* (*Network Access Points*). Jeder, der einen Anschluss an einen der

Tier-1-Provider benötigt, muss wirklich viel Geld dafür zahlen. Untereinander erheben die Tier-1-Provider jedoch keine Gebühren.

Tier-2-Provider besitzen kleinere, regionale Netzwerke und müssen an die Tier-1-Provider zahlen. Die bekanntesten Unternehmen, die Internet-Zugriff für die allgemeine Öffentlichkeit bereitstellen, sind Tier-2-Provider. Tier-3-Provider arbeiten noch regionaler und sind an die Tier-2-Provider angeschlossen.

Möglich wird dieses geschichtete Internet-Konzept erst durch durch sogenannte *Backbone-Router*. Backbone-Router sind mit mehreren anderen Backbone-Routern verbunden, wodurch ein großes, verwobenes Grundgerüst für die Kommunikation entsteht. Abbildung 21.1 veranschaulicht die dezentrale und verwobene Natur des Internets. Der wichtigste Grund für diese Art der Verbindung ist, alternative Datenwege bereitzustellen, falls ein oder mehrere Router ausfallen. Wenn Jane in Houston daher beispielsweise eine Nachricht an ihre Freundin Polly in New York sendet, dann sollte der kürzeste Weg zwischen Jane und Polly im Idealfall der folgende sein: Janes Nachricht stammt von der Rice University in Houston, wird an die Emory University in Atlanta weitergeleitet, geht von da aus zur Virginia University in Richmond und landet schließlich bei SUNY in New York City (Abbildung 21.2) – Polly empfängt die Nachricht und ist glücklich! Das Internet funktioniert wie beabsichtigt.

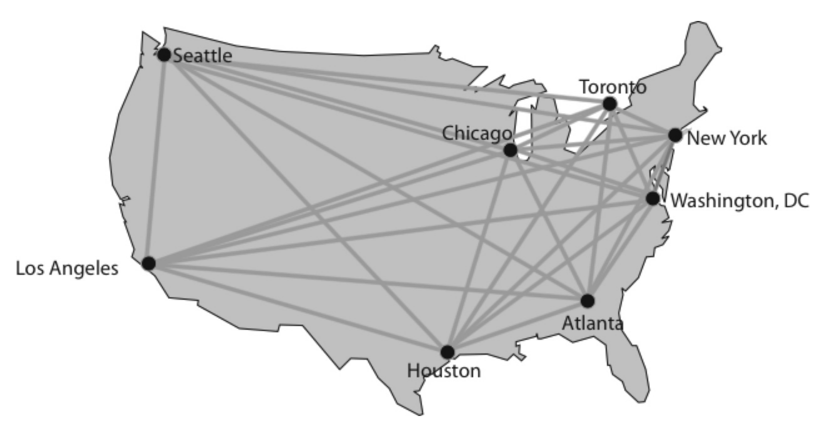


Abb. 21.1: Tier-1-Verbindungen des Internets

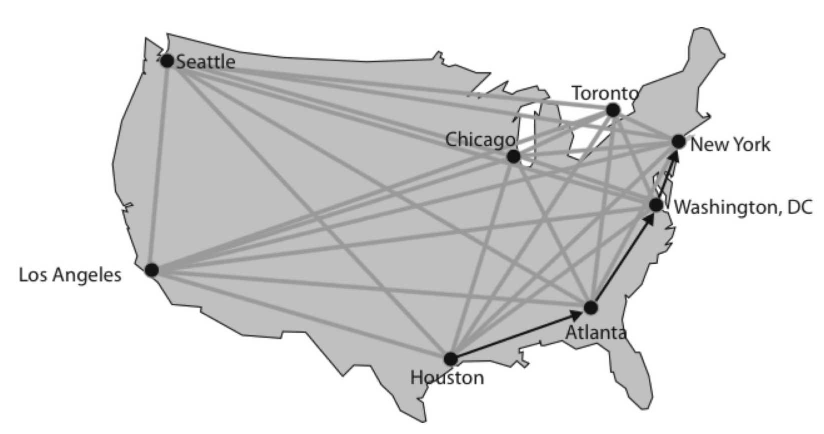


Abb. 21.2: Nachrichtenübermittlung von Houston nach New York

Was geschieht aber, wenn der gesamte Südosten der Vereinigten Staaten einen gigantischen Stromausfall erlebt und alle Staaten von Virginia bis Florida vom Netz gehen? Janes Nachricht würde nun

zurück zur Rice-Uni und den Computern dort gesendet werden. Clever, wie sie sein sollten, würden die Computer die Nachricht nun erneut auf den Weg an Knoten im Netz schicken, die noch funktionieren; sagen wir mal, von Rice zur University of Chicago, anschließend zur University of Toronto und dann zu SUNY (Abbildung 21.3). Und all das gehört im hochredundanten und flexiblen Internet zum Alltag! Das Internet kann heute kaum noch komplett ausfallen – ausgenommen natürlich im Fall einer Katastrophe biblischen Ausmaßes.

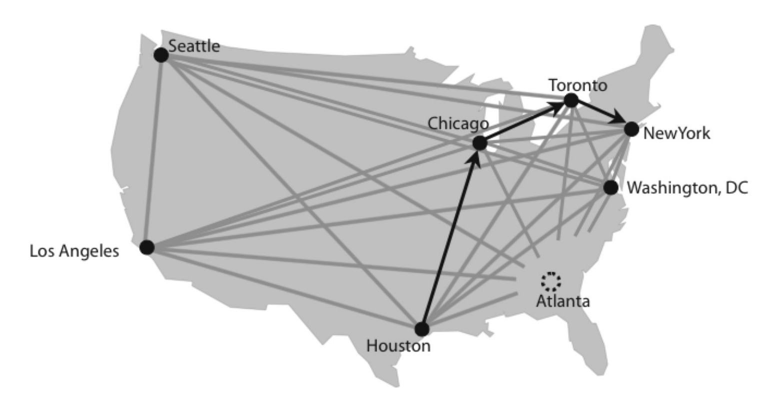


Abb. 21.3: Umgeleitete Nachricht

21.1.2 TCP/IP – die gemeinsame Sprache des Internets

Wie Sie aus früheren Kapiteln des Buches wissen, kann man im Computerbereich mit Hardware allein wenig bewegen. Sie brauchen die Software dazu, um die Maschinen zum Leben zu erwecken und eine Schnittstelle für Menschen zur Verfügung zu stellen. Das Internet bildet da keine Ausnahme. TCP/IP sorgt für die grundlegenden Softwarestrukturen für die Kommunikation über das Internet.

In Kapitel 19, *Lokale Netzwerke*, haben Sie sich bereits ausgiebig mit TCP/IP befasst. Sie sollten daher einen Eindruck von seiner Flexibilität und (was vielleicht noch wichtiger ist) seiner Erweiterbarkeit bekommen haben. TCP/IP sorgt für die Adressierung der Computer, die im Internet miteinander kommunizieren, mit IPv4-Adressen wie etwa 192.168.4.1 oder 16.45.123.7. Als Protokoll ist TCP/IP jedoch weitaus mehr als einfach nur eine Adressierungsmethode. TCP/IP ist das Fundament und die gemeinsame Sprache des Internets. Und es bietet eine enorm offene Grundlage für kreative Erweiterungen. Die Programmierer können Anwendungen schreiben, die sich die TCP/IP-Struktur und dessen Leistungsmerkmale zunutze machen und so etwas wie *TCP/IP-Dienste* entwickeln. Das Beste an den TCP/IP-Diensten ist, dass ihnen nur durch den Erfindungsreichtum der Programmierer eine Grenze gesetzt ist.

Jetzt haben wir es also mit einem enorm großen und wunderbar funktionierenden Netzwerk zu tun. Alle Rootserver, die als Backbones untereinander über redundante Hochgeschwindigkeitsleitungen verbunden sind, und TCP/IP sorgen für Kommunikation und Dienste zum Aufbau sinnvoller Anwendungen, damit die Menschen über große Distanzen hinweg Verbindung miteinander aufnehmen können. Was fehlt nun noch? Natürlich: Wie können Sie sich nun mit diesem großartigen Netzwerk verbinden und seine Vorzüge nutzen?

21.1.3 Internet Service Provider

Nahezu alle Schicht-1- und Schicht-2-Provider vermieten die Verbindungen ins Internet an Unternehmen, die als *ISPs* (*Internet Service Provider*) bezeichnet werden. ISPs sitzen im Wesentlichen an den Ecken im Kernbereich des Internets und zapfen sozusagen den Datenfluss an. Sie wiederum können Verbindungen vom ISP mieten und so ins Internet gelangen.

ISPs gibt es in allen »Größen«. Kabelnetzbetreiber für das Fernsehen, die großen Telefongesellschaften und ähnliche Anbieter haben Millionen von Kunden und ermöglichen es Ihnen, vom lokalen Rechner aus im Web zu surfen. Und dann gibt es auch noch lokale ISPs wie *Electric Power Board* in Chattanooga, Tennessee (Abbildung 21.4). Dieses Unternehmen, das mit dem Spruch »... das schnellste verfügbare Internet. Punkt.« für sich wirbt, bietet seine rasend schnellen Gigabit-Glasfaserverbindungen leider nur den Bewohnern von Chattanooga an, die sich glücklich schätzen dürfen.

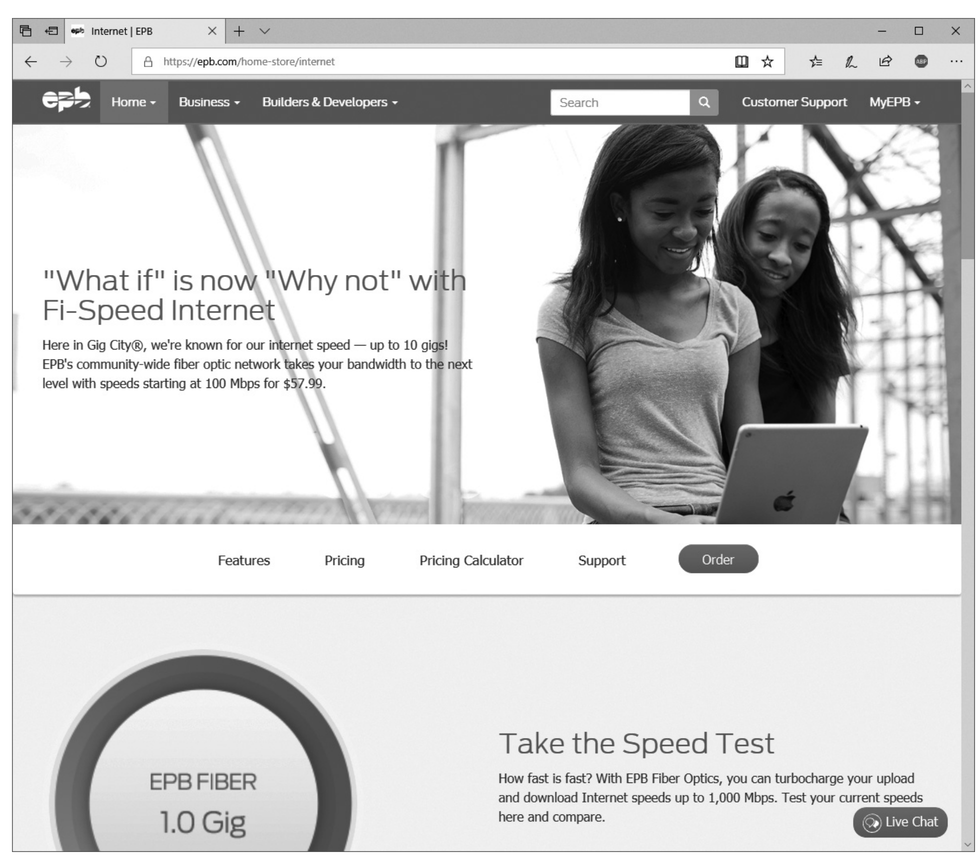


Abb. 21.4: Die Startseite von Electric Power Board

21.1.4 Verbindungskonzepte

Die Verbindung mit einem ISP erfordert zwei Dinge, die aufeinander abgestimmt sein müssen, nämlich die Hardware für die Konnektivität (wie ein Modem und die Telefonleitung) und die Software (Protokolle zum Verwalten der Verbindung und des Datenflusses), die im Betriebssystem konfiguriert werden muss. Außerdem brauchen Sie noch Anwendungen, die die verschiedenen TCP/IP-Dienste nutzen können. Sobald Sie einen Vertrag mit einem ISP geschlossen haben, der Ihnen den Zugang zum Internet bietet, stellt der ISP Ihnen alle nötige Hard- und Software bereit. Bei den meisten ISPs liefert ein Router mit DHCP-Server Ihrem Rechner alle für die Internetverbindung erforderlichen TCP/IP-Konfigurationsdaten. Wie Sie wissen, wird dieser Router als *Standardgateway* bezeichnet. Nach der korrekten Konfiguration Ihrer Software können Sie die Verbindung mit dem ISP herstellen und nun ins weite Internet gehen. Abbildung 21.5 zeigt eine übliche Konfiguration für die Verbindung des Rechners über einen ISP mit dem Internet. Beachten Sie, dass die Verbindung zwischen PC und Standardgateway mit verschiedenen Protokollen und anderer Software verwaltet wird.

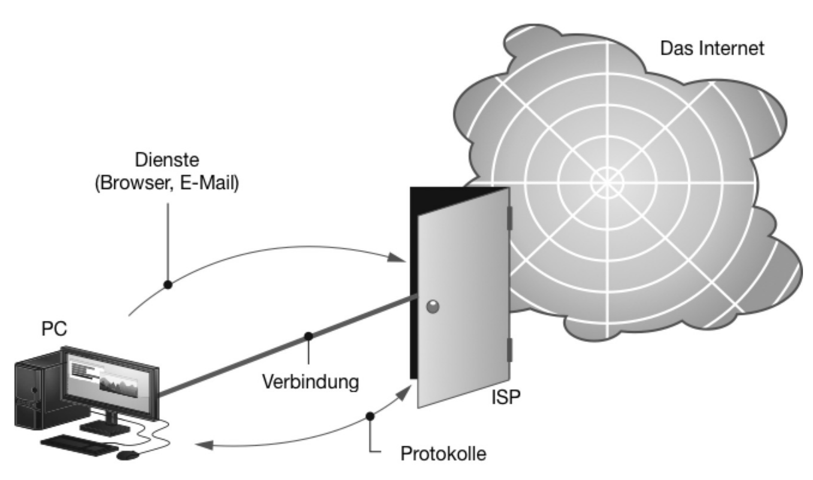


Abb. 21.5: Vereinfachte Darstellung einer Internetverbindung

1001

21.2 Verbindung mit dem Internet herstellen

PCs werden mit einem ISP unter Verwendung von acht verschiedenen Technologien verbunden, die sich in vier Kategorien einteilen lassen:

- analoge und ISDN-Wählverbindungen,
- dedizierte Verbindungen wie DSL, Kabel oder Glasfaser,
- drahtlose Technologien (WLAN und Mobilfunk) und
- Satellitenverbindungen.

Die analoge Wählverbindung ist unter den zur Verfügung stehenden Technologien die langsamste. Sie erfordert eine Telefonleitung und ein spezielles Netzwerkgerät namens Modem. ISDN arbeitet mit digitaler Einwahl und ist schneller. Die übrigen Technologien nutzen normale Ethernet-Netzwerkadapter, die Sie in Kapitel 19, *Lokale Netzwerke*, kennengelernt haben. Wie schnell drahtlose Verbindungen sind, hängt vom betroffenen Gerät und dem verfügbaren Dienst ab. Bei der Satellitenverbindung handelt es sich um einen etwas merkwürdigen Zwitter, denn sie kann in Abhängigkeit von der jeweiligen Konfiguration mit Modem oder Netzwerkkarte genutzt werden, auch wenn zumeist Netzwerkkarten verwendet werden. Schauen wir uns die verschiedenen Verbindungstypen nun der Reihe nach an und werfen wir anschließend einen Blick auf die Router-Konfiguration und die Freigabe von Internetverbindungen.

21.2.1 Wählverbindungen

Eine *Wählverbindung* ins Internet setzt zwei Dinge voraus, nämlich die Hardware zum Anrufen des ISP wie etwa ein Modem oder einen ISDN-Terminaladapter und die Software zum Steuern der Verbindung wie etwa Microsofts DFÜ-Netzwerk. Schauen wir uns als Erstes die Hardware und anschließend die Softwarekonfiguration an.

Modems

In frühen Tagen des Computerzeitalters betrachtete irgendein schlauer Kopf einen telefonierenden Menschen und dann den PC und zählte eins und eins zusammen. Weshalb nicht eine Telefonleitung

zur Datenkommunikation benutzen? Das grundlegende Problem bei diesem Ansatz besteht darin, dass herkömmliche Telefonleitungen mit analogen Signalen, Computer aber mit digitalen Signalen arbeiten (Abbildung 21.6). Ein Einwählnetzwerk setzt ein Gerät voraus, das digitale in analoge Signale verwandeln kann, die dann über die Telefonleitung gesendet und auf der anderen Seite wieder in digitale Signale umgewandelt werden. Genau das leistet ein Modem.

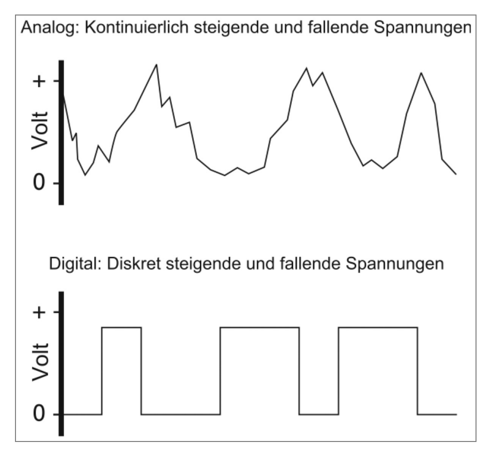


Abb. 21.6: Über Telefonleitungen werden analoge Signale übertragen, während Computer mit digitalen Signalen arbeiten.

Mit *Modems* können Computer miteinander über herkömmliche, kommerzielle Telefonleitungen durch Umwandlung analoger in digitale Signale und umgekehrt kommunizieren. »Modem« ist eine Kurzform von MOdulator/DEModulator und beschreibt die Signalwandlung. Telefonleitungen übertragen Daten in Form analoger Signale über stetige Spannungswechsel. Damit können Computer aber wenig anfangen; sie brauchen digitale Signale, also Spannungen, die entweder anliegen oder nicht anliegen. Computer verwenden aufgrund ihrer binären Natur zwei Spannungszustände, nämlich null Volt und irgendeine (typischerweise niedrige) positive Spannung. Modems übernehmen die analogen Signale aus der Telefonleitung und verwandeln sie in für den PC verständliche digitale Signale (Abbildung 21.7). Und Modems wandeln umgekehrt auch die digitalen Signale des Rechners in analoge Signale für die ausgehende Telefonleitung um.

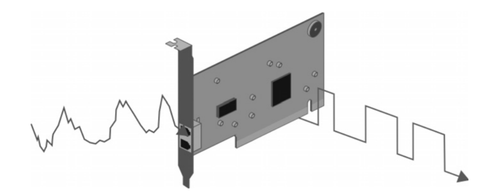


Abb. 21.7: Ein Modem wandelt analoge in digitale Signale um.

Die Geschwindigkeit von Telefonleitungen wird in *Baud* angegeben, womit ein Zyklus pro Sekunde gemeint ist. Eine Telefonleitung kann maximal 2.400 Baud erreichen. Modems können in jedes Baud mehrere Datenbits packen. So enthält beispielsweise bei einem Modem mit einer Geschwindigkeit von 33,6 Kbps (Kilobits pro Sekunde) jedes Baud 14 Bits, was 2.400 x 14 = 33,6 Kbps ergibt.

Hinweis

Modems werden mit einem vierpoligen Stecker per Telefonleitung an eine vierpolige Buchse angeschlossen. Dabei handelt es sich um CAT1-Kabel und RJ11-Stecker/Buchsen.

Der Anschluss oder Einbau von Modems Interne Modems werden ganz anders als externe an den Rechner angeschlossen. Nahezu alle internen Modems werden im Innern des Rechners in einen PCI- oder PCI-Express-Steckplatz eingesetzt (Abbildung 21.8). Aktuelle externe Modems werden über USB mit dem PC verbunden (Abbildung 21.9). USB-Modems unterstützen Plug&Play und lassen sich leicht auch mit unterschiedlichen Rechnern nutzen. Zudem benötigen USB-Modems keine eigene externe Stromversorgung, da sie ihren Strom über die USB-Schnittstelle beziehen.



Abb. 21.8: Ein internes Modem



Abb. 21.9: Ein USB-Modem

DFÜ-Netzwerk

Softwareseitig muss bei DFÜ-Netzwerken das Betriebssystem für die Verbindung mit dem ISP konfiguriert werden. Der ISP stellt eine Telefonnummer, Benutzername und Kennwort zur Verfügung. Außerdem teilt Ihnen der ISP mit, ob Sie im Softwaresetup spezielle Konfigurationsoptionen beachten müssen. Die vollständige Konfiguration eines DFÜ-Netzwerks würde den Rahmen dieses Buches sprengen. Sie sollten aber zumindest wissen, wo Sie die Einstellungen finden, die Sie entsprechend den Angaben des ISPs vornehmen müssen. Dazu wollen wir uns mit dem Applet NETZWERK- UND FREIGABECENTER von Windows 7 ein wenig eingehender befassen.

Netzwerkverbindung einrichten Öffnen Sie in der Systemsteuerung das Applet Netzwerk- und Freigabecenter und wählen Sie im Bereich NETZWERKEINSTELLUNGEN ÄNDERN die Aufgabe NEUE VERBINDUNG ODER NEUES NETZWERK EINRICHTEN aus (Abbildung 21.10).

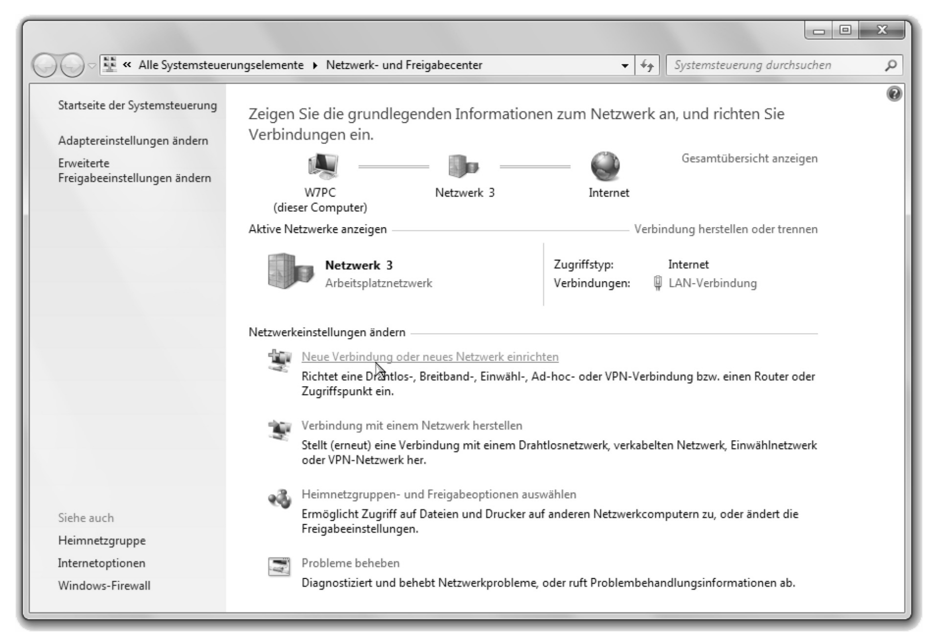


Abb. 21.10: Einrichten einer neuen Verbindung in Windows 7

Wählen Sie auf dem nächsten Bildschirm WÄHLVERBINDUNG EINRICHTEN aus und geben Sie, wie in Abbildung 21.11, Ihre Zugangsdaten ein.

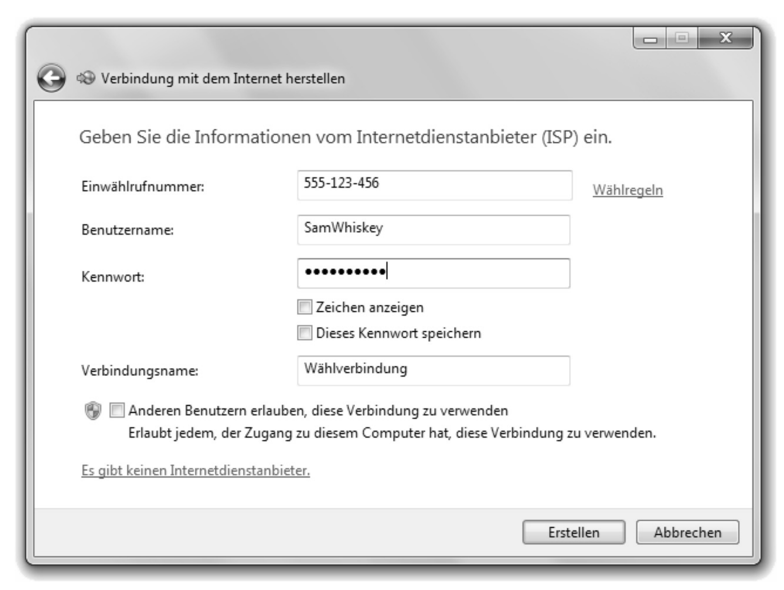


Abb. 21.11: Eingabe der Zugangsdaten unter Windows 7

PPP DFÜ-Verbindungen ins Internet nutzen ein eigenes, spezielles Hardwareprotokoll namens *PPP* (*Point-to-Point-Protocol*). PPP ist ein Streaming-Protokoll, das speziell für Wählverbindungen mit dem

Internet entwickelt wurde. Für Windows ist ein Modem eigentlich nichts anderes als eine spezielle Netzwerkkarte. Unter aktuellen Windows-Versionen können Sie eine neue Einwahlverbindung wie eben beschrieben im NETZWERK- UND FREIGABECENTER konfigurieren.

Die meisten Probleme der Art »Ich komme nicht ins Internet!« haben bei Wählverbindungen mit Anwenderfehlern zu tun. Als Erstes sollten Sie das Modem überprüfen. Schauen Sie sich die Modemeigenschaften an und überprüfen Sie die Einstellung des Lautstärkereglers. Lassen Sie den Anwender dann auf die Verbindungsgeräusche lauschen – ist der Wählton hörbar? Falls nicht, überprüfen Sie, ob die Leitung des Modems richtig an die Telefonbuchse angeschlossen ist. Hört er vielleicht zwar das Modem wählen, aber dann so etwas wie »Ja bitte?!« Falls ja, dann wurde wohl die falsche Nummer gewählt! Die Fehlermeldungen bei falscher Kennworteingabe erklären sich von selbst. Denken Sie auch daran, dass das Kennwort zwar richtig, der Benutzername aber falsch sein kann. Falls die Verbindung immer noch nicht hergestellt werden kann, wird es Zeit, die Netzwerkleute zu rufen, um die DFÜ-Netzwerkeinstellungen überprüfen zu lassen.

ISDN (Integrated Services Digital Network)

Um eine telefonische Verbindung herzustellen, sind einige Komponenten erforderlich. Zunächst einmal haben wir da die Telefonleitung, die vom Telefon zu dem Kasten mit der Netzwerkschnittstelle und von dort zu einem zentralen Switch führt, der der Telefongesellschaft gehört. (Teilweise sind noch weitere Geräte zwischengeschaltet.) Diese zentralen Schaltstellen sind dann untereinander mit *Amtsleitungen* hoher Kapazität verbunden. Vor 1970 war das gesamte Telefonnetz analog. Im Laufe der Zeit begannen dann die Telefongesellschaften damit, ihre Amtsleitungen digital aufzurüsten. Heute ist das gesamte Telefonnetz mit der Ausnahme der Leitung von Ihrem Telefon zur Vermittlungsstelle digital. (Und selbst die ist mittlerweile oft digital.)

Während der Aufrüstung des Telefonnetzes erwarteten die Kunden stets mehr Datendurchsatz für ihre Telefonleitungen. Mit den alten Telefonleitungen ließen sich nicht mehr als 28,8 Kbps erreichen. (56K-Modems, von denen die Telefongesellschaften echt überrascht wurden, gab es erst 1995.) Die Telefonfirmen beeilten sich daher, neue Möglichkeiten für höhere Kapazitäten zu entwickeln. Ihre Lösung war schnörkellos: Das gesamte Telefonnetz sollte digitalisiert werden. Durch zusätzliche spezielle Geräte in den zentralen Vermittlungsstellen und am Standort des Benutzers ließ sich ein Durchsatz von bis zu 64 K je Leitung erreichen, und zwar über die bereits im Telefonnetz verwendeten herkömmlichen Kupferleitungen. Dieses Verfahren zur telefonischen Datenübertragung zwischen den Endstellen über komplett digitale Leitungen wird *ISDN* (*Integrated Services Digital Network*) genannt.

Die ISDN-Dienste arbeiten mit zwei unterschiedlichen Kanälen, den sogenannten B- (*Bearer*) und D-Kanälen (*Delta*). Über die B-Kanäle lassen sich Daten und Sprache mit 64 Kbps übertragen. Über die D-Kanäle werden Steuer- und Konfigurationsdaten mit 16 Kbps übertragen. Bei den meisten ISDN-Anbietern können die Benutzer einen oder zwei B-Kanäle verwenden. Eine häufig verwendete Konfiguration besteht aus zwei B- und einem D-Kanal und wird auch *BRI* (*Basic Rate Interface*) genannt. Sie benutzt nur eine einzige physische Leitung, bei der über die beiden B-Kanäle Daten mit 64 K übertragen werden können, wodurch die Datenrate auf 128 K verdoppelt wird. Mit ISDN lassen sich Verbindungen zudem viel schneller als über Modems herstellen, weil der lange und manchmal nervtötende Verbindungsaufbau bei herkömmlichen Modems entfällt. Die monatlichen Kosten von ISDN-Anschlüssen sind typischerweise etwas höher als bei normalen Telefonanschlüssen. Für die Einrichtung und die benötigten Geräte werden zudem gewisse Gebühren erhoben. Die wesentliche Einschränkung besteht darin, dass ein ISDN-Anschluss normalerweise maximal etwa 5,5 km von einer zentralen ISDN-Vermittlungsstelle entfernt sein darf.

Die physischen ISDN-Verbindungen haben eine gewisse Ähnlichkeit mit den analogen Modemverbindungen. Die ISDN-Steckdose sieht aus wie eine RJ-45-Buchse. Bei der bekanntesten Schnittstelle zum Computer handelt es sich um ein Gerät, das Terminaladapter (TA) genannt wird. Terminaladapter sehen oft ähnlich wie normale Modems aus und sind (wie Modems) in externen und internen Varianten erhältlich. TAs können auch als Hubs angeboten werden, sodass Sie Ihr System damit direkt an Ihr LAN anschließen können.

In den 1990er-Jahren war die Datenübertragungsrate von 128 Kbps eine willkommene Verbesserung im Vergleich zu analogen Modems, heutzutage sind jedoch viel schnellere DSL- und Kabelverbindungen verfügbar, deshalb begegnet man ISDN-Anschlüssen in der Praxis nur noch selten. Sie finden aber noch Verwendung, wenn hohe Anforderungen an die Sicherheit gestellt werden, beispielsweise in militärischen Kommandozentralen.

21.2.2 DSL (Digital Subscriber Line)

DSL (Digital Subscriber Line) als Verbindungstyp zum ISP verwendet eine standardmäßige Telefonleitung, jedoch spezielle Geräte auf jeder Seite, und bietet ständig online geschaltete Internetverbindungen bei rasanten Geschwindigkeiten (insbesondere im Vergleich mit analogen Wählverbindungen). Die Up- und Downloadgeschwindigkeiten der verschiedenen DSL-Varianten unterscheiden sich erheblich. Am unteren Ende des Spektrums werden meist nur einstellige Datenübertragungsraten erzielt – weniger als 1 Mbps beim Upload und rund 3 Mbps beim Download. Neuere DSL-Varianten erreichen Datenübertragungsraten von mehreren Dutzend oder sogar Hunderte Mbps – wenn sie denn verfügbar sind.

Hinweis

Die beiden häufigsten Formen von DSL sind asymmetrisches (ADSL) und symmetrisches DSL (SDSL). ADSL-Leitungen arbeiten mit niedrigeren Uploadgeschwindigkeiten (typischerweise 384, 768 oder 1 Mbps) und höheren Downloadgeschwindigkeiten (zwischen 3 und 16 Mbps). Bei SDSL sind Upload- und Downloadgeschwindigkeiten identisch, es ist aber auch deutlich teurer. Von DSL gibt es eine ganze Menge Varianten mit verschiedenen Leistungsmerkmalen, die zusammenfassend oft als *xDSL* bezeichnet werden.

DSL erfordert benutzerseitig nur wenig Einrichtungsaufwand. Ein Techniker kommt zu Ihnen nach Hause, baut eine Netzwerkkarte in den Internet-PC ein und installiert ein *DSL-Modem* (Abbildung 21.12) und eventuell einen WLAN-Router. Das DSL-Modem wird mit der Telefonleitung und dem PC verbunden (Abbildung 21.13). Wenn Sie auf den Techniker verzichten und sich die Geräte per Post zusenden lassen, brauchen Sie nur ein paar Kabel zusammenzustöpseln und das TCP/IP-Protokoll für die Netzwerkkarte (und gegebenenfalls den Router) zu konfigurieren, damit die Einstellungen mit den vom ISP angegebenen Daten übereinstimmen.



Abb. 21.12: Ein DSL-Modem

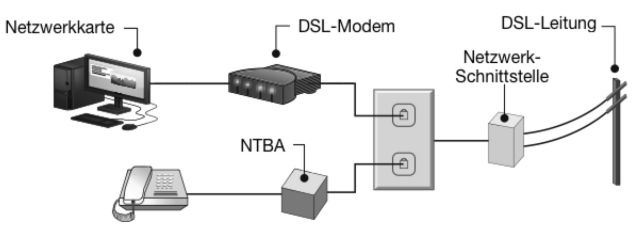


Abb. 21.13: Eine DSL-Verbindung

Das war's! Innerhalb weniger Sekunden können Sie mit dem Surfen im Internet anfangen. Sie benötigen keine zweite Telefonleitung und auch sonst sind keine besonderen Voraussetzungen erforderlich. Die einzige Bedingung besteht darin, dass Sie in der Nähe einer Vermittlungsstelle wohnen müssen, die je nach DSL-Variante einige Hundert Meter oder bis zu etwa 5,5 Kilometer entfernt sein darf.

21.2.3 Kabel

Per Kabel steht eine völlig andere Lösung für hohe Geschwindigkeiten im Internet zur Verfügung, die mit normalen Fernsehkabeln schnelle Verbindungen realisiert. Das Kabel bietet maximale Geschwindigkeiten, die den meisten DSL-Varianten sogar noch etwas überlegen sind. Der Upload erfolgt mit 5 bis 25 Mbps oder mehr und der Download erreicht eine Geschwindigkeit von 15 bis mehr als 1000 Mbps. Kabel-Internetverbindungen stehen theoretisch überall dort zur Verfügung, wo auch Kabel-TV-Anschlüsse angeboten werden.

Zunächst benötigen Sie bei Kabelverbindungen ein RG-6- oder RG-59-Kabel für Ihre Wohnung. Das Kabel wird dann mit einem Kabelmodem verbunden, das wiederum per UTP-Ethernet-Kabel an einen Router oder eine Netzwerkkarte in Ihrem PC angeschlossen wird. Abbildung 21.14 zeigt einen solchen Aufbau.

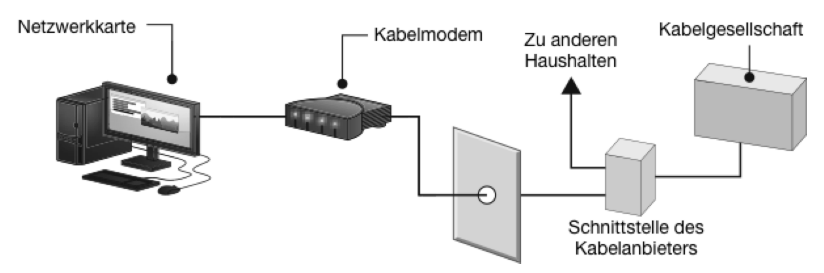


Abb. 21.14: Internetanschluss per Kabelmodem

> **Hinweis**
>
> Die Bedeutung des Begriffs *Modem* hat sich im Bereich moderner Netzwerktechnologien bis zur Unkenntlichkeit gewandelt. Sowohl DSL- als auch Kabel-Internetverbindungen arbeiten vollständig digital. Dennoch wird das Gerät, mit der die eingehenden Signale aus dem Internet empfangen und in für den PC verständliche Daten umgewandelt werden, noch immer als Modem bezeichnet.

21.2.4 Glasfaser

Bis vor Kurzem war Glasfaser so kostspielig, dass nur die wenigsten Leute sich an der superschnellen Geschwindigkeit einer Glasfaserverbindung erfreuen konnten. Inzwischen gibt es jedoch Dienste wie *FTTN* (*Fibre-to-the-Node*) oder *FTTP* (*Fibre-to-the-Premises*), die sich ein Kopf-an-Kopf-Rennen mit den

Angeboten der Kabelanbieter liefern. In jüngster Zeit haben auch Google (mit Google Fiber) und einige lokale Versorgungsunternehmen mit ihren Aktivitäten die Verbreitung von Glasfaserkabeln beschleunigt.

Bei FTTN führt ein Glasfaserkabel vom ISP zu einem Schaltkasten in der Nähe Ihres Hauses. Von dort aus laufen dann herkömmliche Koaxial- oder Ethernet-Kabel bis zu Ihrer Wohnung. Im Fall von FTTP gibt es eine direkte Glasfaserkabelverbindung zwischen ISP und Ihrem Haus oder Büro. Wenn eine solche Leitung verlegt ist, können Sie auch hier Standardkabel oder ein Funknetz verwenden, um sich mit dem Internet zu verbinden.

Der verbreitete Dienst AT&T Internet (ehemals U-verse) beispielsweise bietet eine Downloadgeschwindigkeit von 10 bis 100 Mbps und eine Uploadgeschwindigkeit von 1 bis 20 Mbps (Abbildung 21.15). Verizons Dienst Fios ist der verbreitetste FTTP-Dienst in den USA und bietet Geschwindigkeiten von 50 Mbps bis 1 Gbps – sofern Sie sich das leisten können. Google Fiber bietet ebenfalls eine Up- und Downloadgeschwindigkeit von 1 Gbps.



Abb. 21.15: FTTP-Terminal von AT&T, das hinter meinem Kühlschrank verborgen ist

21.2.5 Drahtlos

Drahtlose Netzwerke nach den 802.11-Standards sind heutzutage so allgegenwärtig, dass die meisten Leute mit dieser Technologie auf das Internet zugreifen. In Cafés, Flughäfen, Schnellrestaurants, Bars usw. gibt es öffentlich zugängliche WAPs. Es gibt sogar einige Städte, die teilweise oder flächendeckend ein drahtloses Netzwerk zur Verfügung stellen.

Hinweis

Ein 802.11-Netzwerk, das eine einzelne Stadt abdeckt, ist ein ausgezeichnetes Beispiel für ein *MAN* (*Metropolitan Area Network*.

In Kapitel 20 wurden drahtlose Netzwerke bereits ausführlich vorgestellt, es gibt daher keinen Grund, die Verbindung mit einem Zugriffspunkt erneut zu erläutern. Denken Sie aber daran, dass die meisten »Hotspots« keinerlei Verschlüsselung bieten, was es für Bösewichte zum Kinderspiel macht, Ihre Internetverbindung abzuhören und alles, was Sie senden und empfangen, mitzulesen.

Vorsicht

Beim Surfen über öffentlich zugängliche Hotspots sollten Sie, falls möglich, HTTPS-geschützte Verbindungen nutzen. Das ist erstaunlich einfach: Geben Sie statt `facebook.com` beispielsweise `https://facebook.com` in Ihren Webbrowser ein oder nutzen Sie eine Browsererweiterung wie *HTTPS Everywhere*, die von der *EFF* (*Electronic Freedom Federation*) angeboten wird.

21.2.6 Richtfunkstrecken

Drahtlose Netzwerke nach dem IEEE-802.11-Standard sind in dicht bevölkerten Gebieten eine brauchbare Alternative für den Internetzugang. Durch die geringe Reichweite ist es aber in Gegenden, in denen das Aufstellen weiterer Zugriffspunkte problematisch ist, nicht praxistauglich. Unter bestimmten Umständen kann das Problem der geringen Reichweite durch leistungsstarke Richtfunkantennen und Ethernet-Netzwerkbrücken behoben werden. Wenn es eine direkte Sichtverbindung zwischen Sender und Empfänger gibt, sind damit Richtfunkstrecken von mehr als zwölf Kilometern Länge möglich. Wenn etwa in einem Wintersportort ein Restaurant in einer Berghütte oder ein Bootshaus am See mit dem Hauptgebäude am Fuße des Berges verbunden werden soll, ist solch eine Richtfunkstrecke eine gut geeignete Lösung. Um größere Datenübertragungsraten zu erzielen, werden höhere Frequenzen des elektromagnetischen Spektrums verwendet. WLAN nutzt Frequenzen von 2,4 oder 5 GHz, wie Sie aus Kapitel 20 wissen, Richtfunkstrecken hingegen nutzen beispielsweise 24 GHz.

21.2.7 Mobilfunk

Wer braucht schon Computer, wenn man mit allen möglichen mobilen Geräten online gehen kann? Nun gut, es gibt noch immer viele Dinge, die sich mit einem Smartphone oder Tablet nicht erledigen lassen. Allerdings unterscheidet sich das mobile Internet dank der Fortschritte hinsichtlich der Datendienste in Mobilfunknetzen immer weniger von dem am heimischen PC.

Wichtig

Mit einer als *Tethering* bezeichneten Methode können Sie die Internetverbindung Ihres Smartphones oder Tablets Ihrem Computer zur Verfügung stellen. Aktivieren Sie den Dienst auf Ihrem Gerät und verbinden Sie es dann mit Ihrem Computer, entweder drahtlos (mobiler Hotspot) oder per USB-Kabel. Die meisten Netzbetreiber verlangen für die Bereitstellung dieses Dienstes eine zusätzliche Gebühr. Ob Ihr Mobilfunkvertrag Tethering erlaubt, müssen Sie bei Ihrem Netzbetreiber in Erfahrung bringen.

Für die verschiedenen mobilen Datendienste hat es im Laufe der Jahre so viele unterschiedliche Bezeichnungen gegeben, dass es eine echte Herausforderung ist, diese alle zu benennen oder gar in eine sinnvolle Reihenfolge zu bringen. Beim Versuch, die Strukturen etwas zu verdeutlichen, hat die Mobilfunkindustrie beim Marketing das Konzept verschiedener Generationen entwickelt: Geräte der ersten Generation werden als 1G bezeichnet, solche der zweiten als 2G, gefolgt von 3G und 4G. Obendrein verwenden verschiedene Technologien Bezeichnungen wie 2,5G, um darauf hinzuweisen, dass es sich nicht mehr um eine 2G-Technologie handelt, aber auch noch nicht ganz um 3G. Diese Bezeichnungen laufen Ihnen ständig über den Weg, insbesondere bei Mobiltelefonen, wenn diese nicht die höchstmögliche Datenübertragungsrate erreichen (Abbildung 21.16). Die Marketingabteilungen neigen dazu, sich die Definition dieser Begriffe in Werbeanzeigen ein wenig zurechtzubiegen. Sie sollten sich daher stets genauer über ein Gerät informieren und nicht nur auf die Generation achten.

Die erste Generation (1G) der Datendienste für Mobiltelefone war noch analog und nicht dafür ausgelegt, Datenpakete zu transportieren. Erst Anfang der 1990er-Jahre setzten sich zwei vollständig digitale Technologien durch, nämlich *GSM* (*Global System for Mobile Communications*) und *CDMA* (*Code Division Multiple Access*). GSM entwickelte sich weiter zu GPRS und EDGE, während CDMA zu EV-DO führte. GPRS und EDGE waren 2,5G-Technologien, EV-DO hingegen schon 3G. Durch Standards

wie UTMS, HSPA+ und HSDPA erreichen auch GSM-basierte Netze das Niveau von 3G und 3,5G. Die in der Praxis erzielbaren Datentransferraten betragen einige Mbps (meist unter 10).



Abb. 21.16: Über 4G verbundenes iPhone

Mittlerweile sind wir bei der vierten Generation angelangt. Die Geräte nutzen nun die seit 2010 verfügbare Technologie namens *LTE* (*Long Term Evolution*), die den Markt dominiert. Schon 2013 hatte LTE in den USA einen Marktanteil von rund 20 Prozent, der in Teilen Asiens sogar noch höher ist, und der Anteil nimmt weiter zu. Mit einer echten 4G-Technologie wie LTE sind (theoretisch) Up- und Downloadgeschwindigkeiten von 100 Mbps bzw. 1 Gbps erreichbar (Abbildung 21.17).

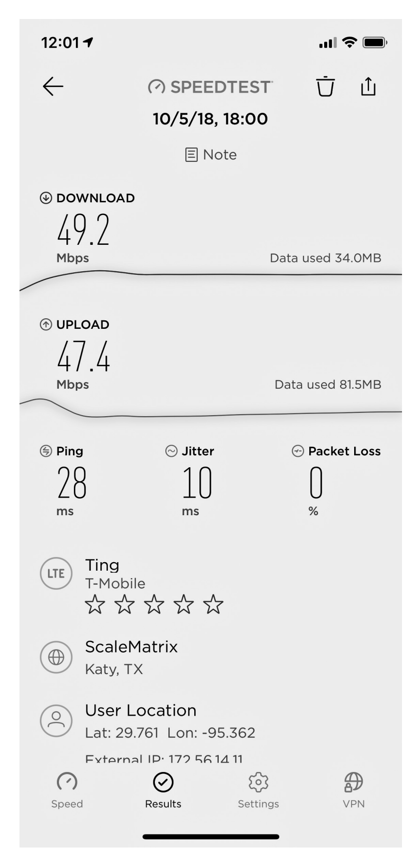


Abb. 21.17: Test der in der Praxis erzielbaren LTE-Geschwindigkeit

Hinweis

LTE und 4G sind inzwischen fast bedeutungsgleich. Gelegentlich sieht man den zusammengewürfelten Begriff »4G LTE«, aber das liegt wohl daran, dass die Marketingabteilungen versuchen, so viele aktuelle Schlagwörter wie möglich unterzubringen.

Mit seiner hohen Geschwindigkeit und flächendeckender Netzabdeckung könnte LTE allmählich drahtgebundene Netzwerktechnologien ablösen. In ländlichen Gegenden kann man seinen Computer mit dem Internet verbinden, ohne auf einen Anschluss per DSL, Kabelnetz oder Glasfaser angewiesen zu sein. Stattdessen verbinden Sie sich mit einem drahtlosen *Hotspot*, einem Gerät, das per Mobilfunk mit dem Internet verbunden ist und diese Verbindung an andere Geräte durchreicht. Hotspots gibt es als eigenständige Geräte, aber auch ein Smartphone kann als Hotspot fungieren. Mehr dazu in Kapitel 24.

Einen Hotspot für den Internetzugang zu verwenden, stellt eine Form des *Tetherings* dar, in diesem Fall eben drahtloses Tethering. Sie können eine Verbindung zu einem Mobilfunkgerät wie einem Smartphone direkt über USB herstellen und die Internetverbindung dieses Geräts für den Internetzugang nutzen (Abbildung 21.18). Hierbei handelt es sich um kabelgebundenes Tethering. Meistens verzichtet man aber auf diese Angabe und spricht einfach nur von Tethering.

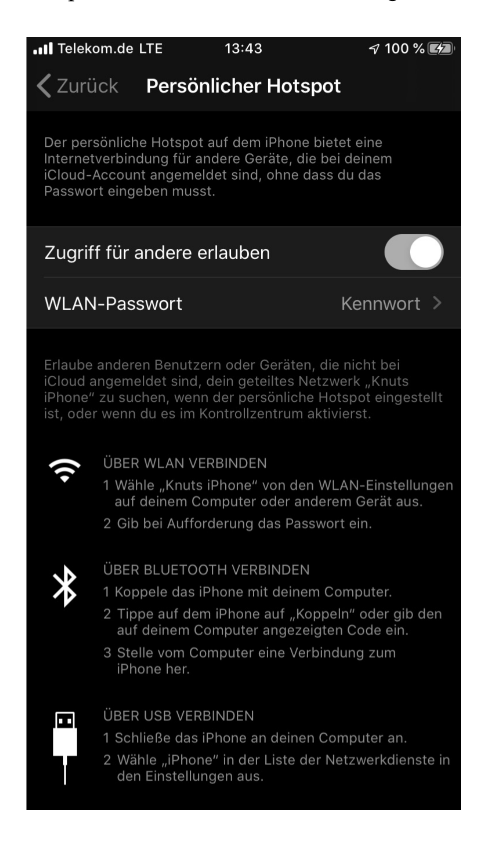


Abb. 21.18: Tethering

Die fünfte Generation der Mobilfunknetze, die sinnvollerweise 5G heißt, hat 2018 bedeutende Verbesserungen erfahren. Sie soll 2019 und 2020 angeboten werden. In den Spezifikationen sind Geschwindigkeiten von bis zu 20 Gbps angegeben – das ist wirklich blitzschnell!

Wichtig

Ebenso, wie es LANs und WANs gibt, spricht man auch von WLANs und WWANs. Ein *WWAN* (*Wireless Wide Area Network*) funktioniert auf die gleiche Wiese wie ein WLAN, verbindet jedoch wie ein WAN mehrere Netzwerke.

21.2.8 Satellit

Satellitenverbindungen ins Internet erhalten die Daten über die an Ihrem Haus oder dem Bürogebäude installierte Satellitenschüssel. Dabei steuert ein Receiver den Datenverkehr und sendet die empfangenen Daten schließlich über ein Ethernet-Kabel an die Netzwerkkarte in Ihrem PC. So weit die Downloadverbindung. Aber was ist hier mit der Uploadverbindung? In den frühen Tagen der Satellitentechnik mussten Sie sich über ein Modem verbinden. Dann standen Ihnen nur die langsamen Modemgeschwindigkeiten von 26 bis 48 Kbps zur Verfügung. Über die Satellitenschüssel hatten Sie dann aber wieder superschnelle Downloads. Es funktionierte ganz gut. Damit können Sie sich sogar in eine Höhle in den Himalaja zurückziehen und immer noch Internet-Konnektivität in DSL-Geschwindigkeit genießen!

Die Satellitentechnik ist wohl von allen Verfahren zur Verbindung mit dem Internet immer noch die aufregendste. Wie auch beim Satellitenfernsehen müssen Sie jedoch eine Satellitenschüssel haben, die genau auf den Satelliten ausgerichtet ist (die Richtung ist von Ihrem Standort abhängig). Von der Satellitenschüssel führt ein Koaxialkabel zum Satellitenempfänger, der einen RJ-45-Anschluss besitzt. An diesem können Sie per Patchkabel Ihren Computer oder Router anschließen. Die Geschwindigkeit liegt bei ca. 25 Mbps (Download) und 3 Mbps (Upload).

Der Internetzugang per Satellit hat ein paar Nachteile. Die Laufzeit der Signale über die zurückzulegende Distanz führt zu kleinen Verzögerungen, die *Satelliten-Latenz* genannt werden. Diese Latenz ist im Allgemeinen zu vernachlässigen, es sei denn, die Signalqualität nimmt bei schlechtem Wetter (Regen und Schnee) deutlich ab. Echtzeitanwendungen wie Spiele oder Videochats können dadurch beeinträchtigt werden. Darüber hinaus implementieren die meisten Anbieter Nutzungsbeschränkungen, um eine Überlastung des Systems zu verhindern, die insbesondere die Hauptnutzungszeit betrifft.

21.2.9 Internetverbindung gemeinsam nutzen

Nun haben Sie sich also die Zugangsdaten für einen Internetzugang beschafft und möchten sich natürlich sofort verbinden. Es gibt hier zwei Möglichkeiten:

1. Einen einzelnen Computer mit dem Internet verbinden
2. Ein Netzwerk mit dem Internet verbinden

Einen einzelnen Computer mit dem Internet zu verbinden, ist ganz einfach. Wenn Sie einen WLAN-Router verwenden, müssen Sie nur die vom ISP gelieferten Zugangsdaten eintragen, um ihn mit dem Internet zu verbinden. Allerdings wird jeder anständige Techniker auch die in Kapitel 20 beschriebenen Maßnahmen durchführen, um das drahtlose Netzwerk zu schützen. Wenn Sie lieber ein kabelgebundenes Netzwerk einrichten möchten, müssen Sie von Ihrem Gerät zum PC ein Kabel verlegen.

Zum Verbinden mehrerer Computer per Kabel sind kleine Router gut geeignet. Etliche Hersteller bieten robuste und einfach zu konfigurierende Hardwarelösungen an, über die mehrere Computer eine einzige Internetverbindung nutzen können. Diese kleinen Kistchen erfordern nur wenig Konfigurationsaufwand und sorgen obendrein auch für einen gewissen Firewall-Schutz zwischen den Rechnern im LAN und dem Internet. Mehr über Firewalls erfahren Sie in Kapitel 27, *Computersicherheit*. Letztlich müssen Sie zur Installation eines solchen Routers einfach nur Ihren Rechner mit einem der LAN-Anschlüsse an dessen Rückseite verbinden und dann das Kabel der Internetverbindung an die Buchse mit der Beschriftung Internet oder WAN anschließen.

Es gibt buchstäblich Hunderte einwandfrei funktionierende, kleinformatige DSL/Kabel-Router für kleine Büros oder Heimnetzwerke (Abbildung 21.19). So ein Gerät besitzt typischerweise vier Ether-

net-Anschlüsse für LAN-Computer und kann auch als WAP konfiguriert werden und so für den drahtlosen Internetzugang sorgen. Der Router verwendet, wie ähnliche Geräte auch, *NAT* (*Network Address Translation*) und übersetzt die internen LAN-Adressen in jene, die für den Internetzugriff benutzt werden. Mit NAT werden alle Computer im LAN für das Internet zu einem einzigen Rechner. Dadurch werden Ihre Rechner auch vor dem Internet versteckt und sind in diesem für andere Computer nicht sichtbar. Alles, was irgendjemand im Internet sehen kann, ist Ihre *öffentliche* IP-Adresse. Dabei handelt es sich um die vom ISP zugewiesene Adresse, während für alle Rechner in Ihrem LAN *private* IP-Adressen verwendet werden, die für die Außenwelt unsichtbar sind. NAT arbeitet daher als Firewall und schützt Ihr internes Netzwerk vor Eindringlingen und äußeren Gefahren.



Abb. 21.19: WLAN-Router

Wichtig

Dank dynamischen NAT können sich mehrere Computer eine bestimmte Anzahl verfügbarer öffentlicher IP-Adressen miteinander teilen. Beispielsweise könnten nur zehn IP-Adressen für 40 PCs im LAN verfügbar sein. Der LAN-Datenverkehr nutzt die internen, privaten IP-Adressen. Möchte nun ein PC auf Daten außerhalb des Netzwerks zugreifen, vergibt DNAT zu diesem Zweck eine der verfügbaren IP-Adressen aus dem vorhandenen Adresspool. (DNAT wird manchmal auch als Pool-NAT bezeichnet.)

Das funktioniert auch tadellos – es sei denn, Sie sind der Elfte, der versucht, auf das Internet zuzugreifen. Der Nachteil ist natürlich, dass man trotzdem eine Reihe teurer öffentlicher IP-Adressen benötigt.

Grundlegende Router-Konfiguration

Die kleinen Router erfordern nur sehr wenig Konfigurationsaufwand und funktionieren oft schon im Auslieferungszustand problemlos (wenn auch nicht selten völlig ungesichert), wenn sie lediglich eine gemeinsame Internetverbindung bereitstellen sollen. Manchmal bekommen Sie es aber mit komplexeren Netzwerken zu tun, für die Sie die Router-Einstellungen anpassen müssen. Die allermeisten dieser Router besitzen einen integrierten Webserver mit Webseiten zur Konfiguration, auf die Sie zugreifen können, wenn Sie die IP-Adresse des Routers in die Adresszeile eines Webbrowsers eingeben. Die vorkonfigurierte Adresse unterscheidet sich bei den verschiedenen Modellen und Herstellern, ist aber in jedem Fall in der Dokumentation des Routers zu finden. Es wird dann ein Dialogfeld angezeigt, das Sie zur Eingabe von Benutzernamen und Kennwort für den Router auffordert (Abbildung 21.20). Wie die IP-Adresse unterscheiden sich auch die vorkonfigurierten Benutzernamen und Kennwörter bei den verschiedenen Modellen und Herstellern. Wenn Sie die korrekten Daten eingegeben haben, werden Sie von der Hauptseite des Router-Konfigurationsprogramms begrüßt (Abbildung 21.21). Hier können Sie alle Router-Einstellungen ändern.

Wichtig

Viele für Privathaushalte gedachte Geräte besitzen eine Funktion namens *Universal Plug and Play* (*UPnP*), die es ihnen gestattet, im Netzwerk nach anderen UPnP-Geräten zu suchen und sich automatisch mit die-

sen zu verbinden. Diese Funktion erlaubt zwar eine problemlose Verbindungsaufnahme, aber zum Preis etwas niedrigerer Sicherheit.



Abb. 21.20: Der Router fordert zur Eingabe von Benutzernamen und Kennwort auf.

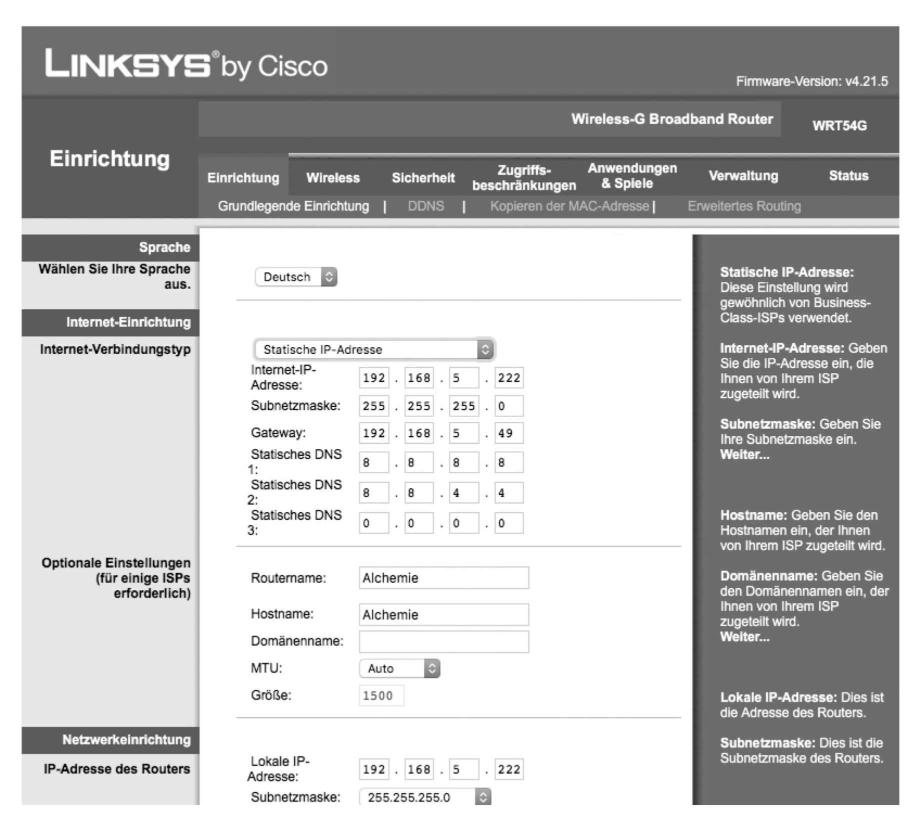


Abb. 21.21: Startseite zur Konfiguration eines Routers

Wenden wir uns nun einigen der grundlegenden Einstellungen zu, die Ihnen für die CompTIA-Prüfungen vertraut sein sollten. In Kapitel 27, *Computersicherheit*, werden wir einen Blick auf einige erweiterte Einstellungen werfen, die den Computer bei der Nutzung von Internetdiensten schützen.

Benutzername und Kennwort ändern Eine der ersten Aufgaben, die Sie bei Ihrem betriebsbereiten Router erledigen sollten, ist die Änderung von Benutzername und Kennwort, damit diese nicht mehr der Werksvorgabe entsprechen. Wie Sie aus Kapitel 20, *Drahtlose Netzwerke*, wissen, ist das insbesondere wichtig, wenn Sie beliebige drahtlose Zugriffe zulassen. Wenn Sie es bei Benutzernamen und Kennwort bei den Voreinstellungen belassen, kann jeder mit Zugang zu Ihrem LAN leicht auf den Router zugreifen und dessen Einstellungen abwandeln. Erfreulicherweise machen es die Router-Hersteller dem Benutzer leicht, die Zugangsdaten wie in Abbildung 21.22 zu ändern.



Abb. 21.22: Ändern der Zugangsdaten des Routers

Einstellung statischer IP-Adressen Wenn Sie sich um die Zugangsdaten gekümmert haben, können Sie sich der Einrichtung des Routers für die Verwendung einer statischen IP-Adresse für das Internet oder die WAN-Verbindung zuwenden. In den meisten Fällen schließen Sie den Router an die Internetverbindung (WAN) an, und er erhält über DHCP wie jeder andere Computer eine IP-Adresse vom ISP zugewiesen (dynamische IP-Adresse). Natürlich bedeutet dies, dass sich Ihre Internet-IP-Adresse von Zeit zu Zeit ändert, was ein gewisser Nachteil sein kann. Die meisten Benutzer stört das nicht weiter, aber für einige Heimanwender und Unternehmen kann das ein Problem darstellen. Um dieses Problem zu lösen, können Sie bei den meisten ISPs (oft für eine monatliche Gebühr) auch eine statische IP anfordern. Wenn Ihnen Ihr ISP eine statische IP-Adresse zugewiesen hat, müssen Sie diese manuell in Ihrem Router eintragen. Das geschieht auf demselben Weg wie bei den bisher betrachteten Änderungen. Bei meinem Router gibt es eine Registerkarte zur WAN-Konfiguration, auf der ich alle Einstellungen gemäß den Angaben meines ISPs vornehmen kann (Abbildung 21.23).

IP-Einstellungen
Internet-IP-Adresse: 280 . 168 . 45 . 35
Subnetzmaske: 255 . 255 . 255 . 0
Standard-Gateway: 280 . 168 . 45 . 40
Primärer DNS: 280 . 170 . 38 . 35
Sekundärer DNS: 280 . 170 . 28 . 36

Optionale Einstellungen (für einige ISPs erforderlich)
Host-Name:
Domänenname:
MTU: Auto
Größe: 1500

Abb. 21.23: Einstellungen zur Verwendung einer statischen IP-Adresse

Denken Sie daran, dass Sie Ihren Verbindungstyp ändern müssen (von Automatisch/DHCP auf Statische IP), um die neuen statischen Adressen eingeben zu können

Firmware aktualisieren

Router unterschieden sich insofern nicht von anderen Computern, dass sie Programme ausführen. Da Software aber Bugs, Schwachstellen und andere Probleme aufweisen kann, muss sie möglicherweise von Zeit zu Zeit aktualisiert werden. Die Router-Hersteller sprechen hier von *Firmware-Updates* oder *Firmwareaktualisierungen* und stellen sie entweder auf einer der Konfigurationsseiten des Routers oder auf ihren Webseiten zum Download bereit.

Hinweis

Das Erwähnte trifft für kommerziell erhältlich Router im Allgemeinen zu. Manche vom ISP bereitgestellten Router aktualisieren sich jedoch womöglich automatisch.

Falls Ihr Router die direkte Aktualisierung auf einer der Konfigurationsseiten anbietet, sind Sie nur ein paar Mausklicks von der Aktualisierung entfernt. Andernfalls müssen Sie nur die aktuelle Firmware von der Website des Herstellers auf Ihren Rechner herunterladen. Dann rufen Sie die Konfigurationsseiten des Routers im Webbrowser auf und machen die Seite zum Firmware-Upload ausfindig. Bei meinem Router sieht sie wie in Abbildung 21.24 aus. Anschließend folgen Sie den Anweisungen und klicken abschließend *Update* oder *Aktualisieren* an. Dabei sollten Sie aber Vorsicht walten lassen, denn anders als Windows-Updates können missglückte Firmware-Aktualisierungen Ihren Router in einen nutzlosen Ziegelstein verwandeln. Das geschieht zwar sehr selten, Sie sollten es dennoch nicht vergessen, wenn Sie Firmware-Updates vornehmen.

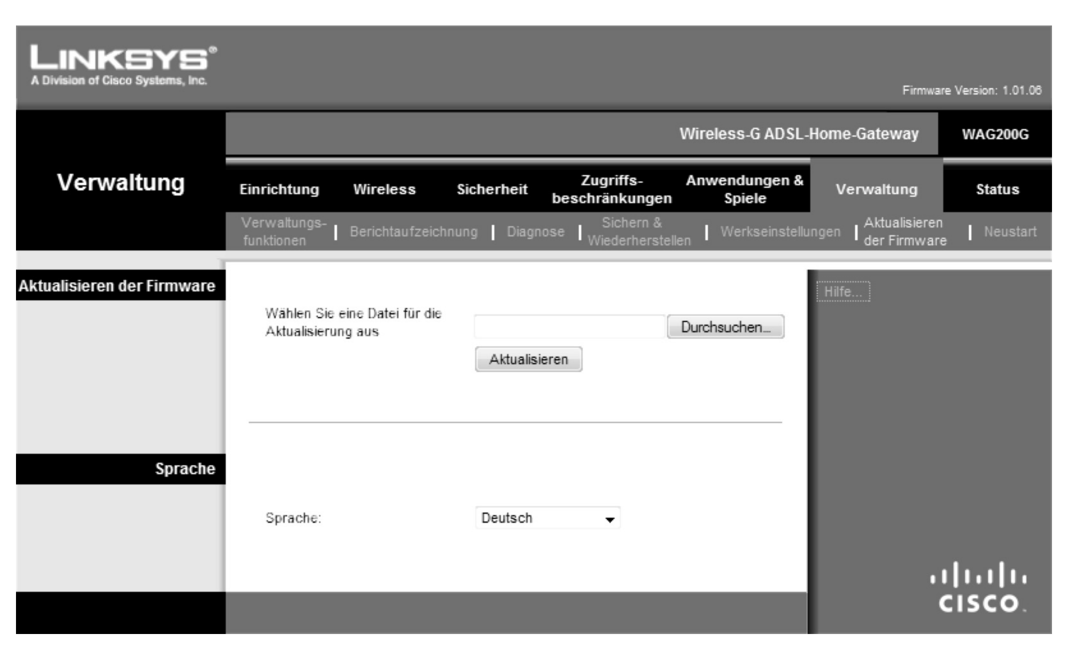


Abb. 21.24: Aktualisieren der Firmware

21.3 Anwendungsprotokolle

Sobald Sie eine Verbindung zum Internet hergestellt haben, brauchen Sie zur Nutzung der verschiedenen TCP/IP-Dienste bestimmte Anwendungen. Um im Web zu surfen, benötigen Sie einen Webbrowser, wie Mozilla Firefox, Google Chrome oder Microsoft Edge. Wenn Sie einen VoIP-Anruf

tätigen möchten, ist dazu eine Software wie Skype oder Google Voice erforderlich. Diese Anwendungen nutzen ihrerseits klar voneinander abgegrenzte Anwendungsprotokolle. Alle Webbrowser verwenden *HTTP* (*Hypertext Transfer Protocol*), alle E-Mail-Programme verwenden *POP3* (*Post Office Protocol 3*) oder *IMAP4* (*Internet Message Protocol 4*) zum Empfangen bzw. *SMTP* (*Simple Mail Transfer Protocol*) zum Versenden von E-Mails usw. Jedem Internetprotokoll ist eine eigene Portnummer zugeordnet und es gelten jeweils eigene Regeln. Zwar gibt es mehrere Zehntausend verschiedene Internetprotokolle, aber für die CompTIA-Prüfungen müssen Sie nur einige wenige der wichtigsten Anwendungsprotokolle kennen. (SFTP und VoIP sind in den Lernzielen nicht aufgeführt, ich führe Sie der Vollständigkeit halber dennoch auf.)

- World Wide Web (HTTP und HTTPS)
- E-Mail (POP3, IMAP4 und SMTP)
- Telnet
- SSH
- FTP/SFTP
- Remote Desktop Protocol (RDP)
- VoIP (SIP)

Neben diesen alltäglich genutzten, augenfälligen Anwendungsprotokollen gibt es auch Hunderte oder vielleicht Tausende davon, die hinter den Kulissen ihre wichtigen Aufgaben erledigen und dafür sorgen, dass die Anwendungsprotokolle, die wir bewusst nutzen, einwandfrei arbeiten. Ihnen sind in Kapitel 19 bereits einige dieser versteckten Anwendungsprotokolle begegnet. Nehmen wir beispielsweise DNS, ohne dass es nicht möglich wäre, im Webbrowser einfach `www.google.com` einzugeben, oder DHCP, von dessen Arbeit Sie ebenfalls nichts bemerken, aber ohne DHCP erhielten die Computer, die das Protokoll verwenden, keine IP-Adressen.

Ein weiteres Beispiel: Niemand möchte aus Angst vor Hackern Kreditkartendaten, private Telefonnummern oder andere persönliche Daten ungeschützt über das Internet übertragen. Glücklicherweise gibt es Methoden zum Verschlüsseln dieser Informationen. Am häufigsten wird dazu *HTTPS* (*Hypertext Transfer Protocol Secure*) eingesetzt. Aus Sicht des Webbrowsers sind HTTPS und HTTP einander sehr ähnlich, HTTPS nutzt jedoch Port 443 statt Port 80. Ob eine Website HTTPS verwendet, ist leicht daran erkennbar, dass die Internetadresse, wie in Abbildung 21.25, mit `https` statt nur mit `http` beginnt. Sie müssen sich bei HTTPS um nichts weiter kümmern, es funktioniert im Webbrowser automatisch.

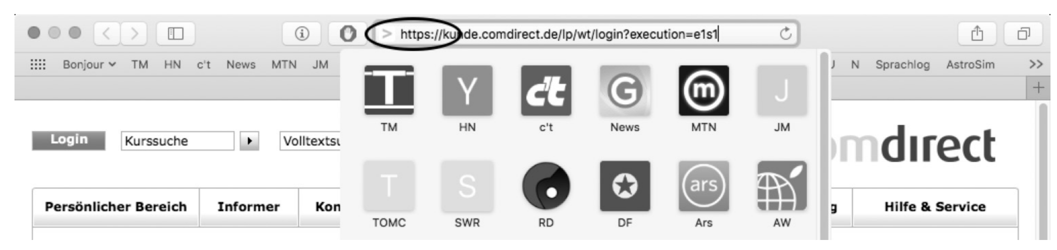


Abb. 21.25: Eine sichere Webseite

Um die sichtbaren Anwendungsprotokolle von den unsichtbaren zu unterscheiden, werde ich den Begriff »Dienstprotokolle« für die im Hintergrund arbeitenden Anwendungsprotokolle verwenden. Demnach ist HTTP ein Anwendungsprotokoll und DNS ein Dienstprotokoll. Alle TCP/IP-Protokolle verwenden eine festgelegte Portnummer und benötigen zur Nutzung eine Anwendung, für die jeweils spezielle Einstellungen erforderlich sind. Sie werden eine Reihe dieser Dienste kennenlernen und konfigurieren. Tabelle 21.1 und Tabelle 21.2 geben Ihnen einen schnellen Überblick über Name, Funktion und Portnummer der Anwendungs- bzw. Dienstprotokolle, die Sie für die CompTIA-Prüfungen besser kennen sollten.

TCP/IP-Dienst	Funktion	Portnummer
HTTP	Webseiten	80
HTTPS	Sichere Webseiten	443
FTP	Dateitransfer	20, 21
SFTP	Sicherer Dateitransfer	22
IMAP4	Eingehende E-Mail	143
POP3	Eingehende E-Mail	110
SMTP	Ausgehende E-Mail	25
Telnet	Terminalemulation	23
SSH	Verschlüsselte Terminalemulation	22
RDP	Remote Desktop	3389
SIP	Voice over IP	5060

Tabelle 21.1: Portnummern von Anwendungsprotokollen

TCP/IP-Dienst	Funktion	Portnummer
DNS	Verwendung von DNS-Namen	53 (UDP)
DHCP	Automatische IP-Adresszuweisung	67, 68 (UDP)
LDAP	Verzeichnisdienste abfragen	389 (TCP)
SNMP	Entfernte Verwaltung von Netzwerkgeräten	161, 162 (UDP)
SMB	Datei- und Druckerfreigaben	445 (TCP), 137, 138, 139 (UDP)
AFP	Dateifreigaben in macOS	548 (TCP)
SLP	Service Location Protocol	427 (TCP/UDP)
NetBIOS/NetBT	NetBIOS über TCP/IP	137, 138, 139 (TCP/UDP)

Tabelle 21.2: Portnummern von Dienstprotokollen

Hinweis

Es ist wichtig, zu wissen, welche Protokolle und welche Ports eine Anwendung nutzt. Lesen Sie gegebenenfalls in Kapitel 19 nach. Dort wird auch NetBIOS erläutert.

Nach der Vorstellung dieser Protokolle geht es um virtuelle private Netzwerke (*VPN – Virtual Private Networks*).

Wichtig

Die in Tabelle 21.1 und Tabelle 21.2 aufgeführten Protokolle sollten Sie für die CompTIA A+-Prüfung 1001 kennen.

1002

21.3.1 Das World Wide Web

Das Web sorgt für die grafische Oberfläche des Internets. Webserver sind Rechner, auf denen spezielle Programme ausgeführt werden und die im weitesten Sinne Websites und Webseiten anbieten, auf die Sie unter Verwendung des HTTPS-Protokolls über Port 43 oder des HTTP-Protokolls über Port 80 zugreifen können und die mit mehr oder weniger sinnvollen Informationen glänzen. Mit speziellen Programmen wie etwa Apple Safari, Microsoft Edge, Google Chrome oder Mozilla Firefox klicken Sie Links auf einer Webseite an und werden unverzüglich mit beliebigen Webservern auf der ganzen Welt verbunden. Abbildung 21.26 zeigt Firefox mit der Homepage der Website meines Unternehmens `www.totalsem.com`). Wo befindet sich dieser Server? Spielt das denn eine Rolle? Er könnte in einem Kämmerchen in meinem Büro oder in einem Rechenzentrum in Kanada stehen. Das Schöne am Web ist, dass Sie mit ein oder zwei Mausklicks an jede beliebige Stelle im Internet und die gewünschten Informationen gelangen können.

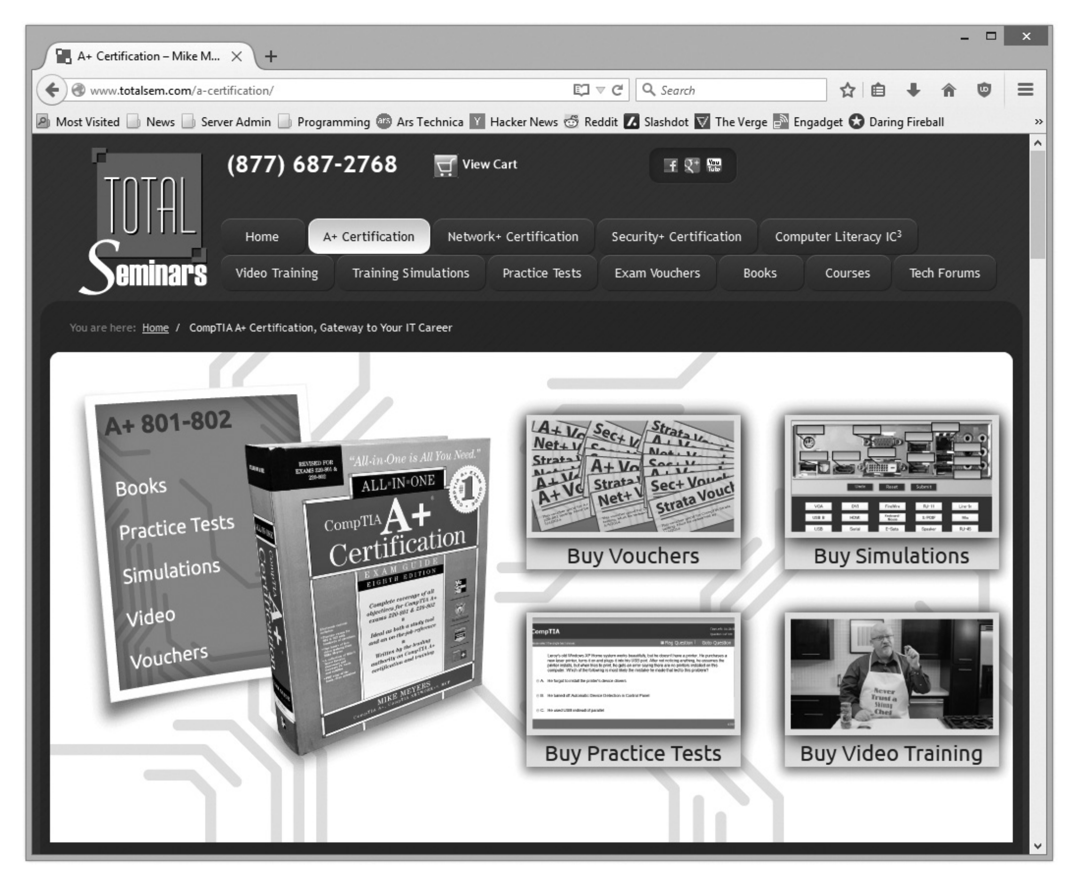


Abb. 21.26: Anzeige einer Webseite in Mozilla Firefox

Die Einrichtung eines Webbrowsers macht so gut wie keine Mühe. Solange die Internetverbindung funktioniert, arbeiten die Webbrowser nahezu automatisch. Das soll nicht heißen, dass es nicht zahlreiche Einstellmöglichkeiten für sie gibt – die Standardeinstellungen sind aber fast immer angemessen.

Wenn Sie beispielsweise eine Webadresse eintippen wie diejenige der weltweit wohl beliebtesten Suchmaschine (`www.google.de`) und das nicht funktioniert, dann sollten Sie die Leitung und Ihre Netzwerkeinstellungen überprüfen. Sicher finden Sie das Problem schnell heraus.

Internet Explorer konfigurieren

Webbrowser lassen sich umfassend konfigurieren. Bei den meisten Webbrowsern können Sie die standardmäßige Schriftartgröße einstellen, auswählen, ob er Grafiken anzeigen soll oder nicht, sowie verschiedene andere Einstellungen vornehmen. Obwohl alle Webbrowser diese Einstellungen anbieten, finden Sie diese an manchmal völlig unterschiedlichen Stellen. Falls Sie mit dem älteren Internet Explorer (IE) arbeiten, der zusammen mit Windows-Versionen bis 8.1 ausgeliefert wird, dann finden Sie die entsprechenden Konfigurationswerkzeuge im Applet INTERNETOPTIONEN in der Systemsteuerung oder im Menü EXTRAS (Abbildung 21.27).

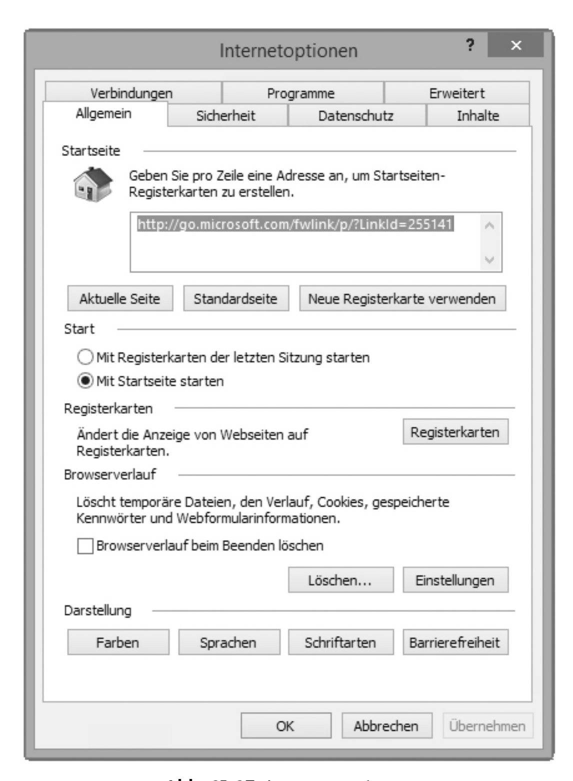


Abb. 21.27: Internetoptionen

Ich finde es befremdlich, dass die CompTIA in den Lernzielen ausdrücklich die INTERNETOPTIONEN erwähnt. Wie Sie wissen, gibt es auch andere Browser. Ich werde daher zunächst anhand des Internet Explorers die üblicherweise vorhandenen Optionen erläutern und die Diskussion dann auf andere Webbrowser ausdehnen.

Nach dem Öffnen der Internetoptionen werden sieben Registerkarten angezeigt. Auf der ersten Registerkarte ALLGEMEIN werden die grundlegenden Einstellungen vorgenommen: Startseite, der Verlauf sowie weitere, das Erscheinungsbild betreffende Einstellungen. Hier können Sie beispielsweise ändern, wo die besuchten Webseiten gespeichert werden bzw. diese löschen.

Die Registerkarte SICHERHEIT ermöglicht es Ihnen festzulegen, in welchem Maße der Internet Explorer Sie beim Surfen schützt (Abbildung 21.28). Sie können hier Vorgaben für die verschiedenen Zonen

(Internet, lokales Intranet, vertrauenswürdige und eingeschränkte Sites) machen und Websites den verschiedenen Zonen zuordnen. Nach Auswahl einer Zone können Sie die Sicherheitsstufe anpassen, wobei eine hohe Sicherheitsstufe mehr Websites blockiert und bestimmte Plug-ins deaktiviert, während bei mittlerer und niedriger Sicherheitsstufe auch weniger sichere Websites angezeigt und deren Funktionen ausgeführt werden.



Abb. 21.28: Die Registerkarte SICHERHEIT

Die Registerkarte DATENSCHUTZ funktioniert auf ganz ähnliche Weise, kontrolliert jedoch die Privatsphäre betreffende Daten, wie Cookies, Popups oder Ortungsdienste und ob Browser-Erweiterungen ausgeführt werden. Mit einem Schieberegler legen Sie fest, was genau blockiert wird. Bei der höchsten Einstellung werden sämtliche Cookies blockiert, bei der niedrigsten hingegen keine. Ändern Sie diese Einstellung, wenn Ihnen die Vorstellung nicht gefällt, dass Websites Ihren Browser-Verlauf verfolgen. (Manche Cookies haben allerdings auch andere Aufgaben, beispielsweise die Authentifizierung eines Benutzers.)

Auf der Registerkarte INHALTE steuern Sie, was Ihnen der Browser anzeigt und was nicht. Dabei werden die Inhalte mittels Zertifikaten und eines Werkzeugs namens FAMILY SAFETY gefiltert, das es Administratoren erlaubt, den Zugriff auf Websites, Glücksspiele, Drogenmissbrauch und andere Dinge anhand von Bewertungssystemen und Ausnahmelisten einzuschränken. Es ist sogar möglich, den Zugriff zeitlich zu begrenzen. Hier können Sie außerdem die Auto-Vervollständigung anpassen, die Internetadressen für Sie ergänzt, oder RSS-Feeds konfigurieren.

Auf der Registerkarte VERBINDUNGEN können Sie gleich eine ganze Reihe von Dingen erledigen: Internetverbindung per Breitband oder als Einwahl konfigurieren, Verbindung zu einem VPN herstellen, einen Proxyserver einrichten oder einzelne LAN-Einstellungen ändern (obwohl Sie das kaum

benötigen werden). Proxyserver sind ein wenig kompliziert, aber die CompTIA verlangt von Ihnen, dass Sie sich damit auskennen.

Viele Unternehmen verwenden einen *Proxyserver*, um den Internet-Zugang ihrer Angestellten zu filtern. Wenn Sie im Unternehmensnetzwerk arbeiten, müssen Sie Ihre Proxy-Einstellungen im Webbrowser (oder etwaiger anderer Internet-Software) festlegen. Ein Proxyserver ist eine Software, die das Durchleiten mehrerer Verbindungen ins Internet durch einen geschützten PC ermöglicht. Anwendungen, die auf Internetressourcen zugreifen wollen, senden Anforderungen an den Proxyserver, anstatt direkt auf das Internet zuzugreifen, wodurch die Client-Rechner geschützt werden und der Netzwerkadministrator Internetzugriffe überwachen und beschränken kann. Alle Anwendungen müssen daher so konfiguriert werden, dass sie den Proxyserver verwenden.

Die nächste Registerkarte PROGRAMME enthält Einstellungen hinsichtlich des Standardbrowsers, aktivierter Erweiterungen (wie z.B. Java) und legt fest, wie andere Programme mit HTML-Dateien oder E-Mail-Nachrichten umgehen.

Auf der Registerkarte ERWEITERT findet sich erwartungsgemäß ein Haufen erweiterter Einstellungen, die größtenteils durch das Markieren eines Kontrollkästchens ein- oder ausgeschaltet werden (Abbildung 21.29). Unter anderem sind hier Optionen zu Eingabehilfen, Browsing, Multimedia und am wichtigsten, zur Sicherheit verfügbar. Neben vielen anderen möglichen Einstellungen legen Sie hier fest, wie der Internet Explorer die Zertifikate von Websites überprüft. Außerdem gibt es die Möglichkeit, die Einstellungen zurückzusetzen, falls Sie von vorne anfangen möchten.

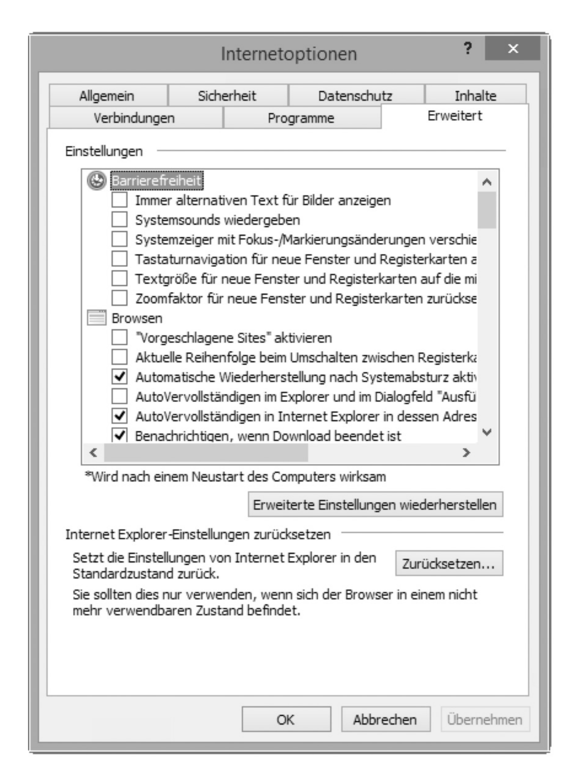


Abb. 21.29: Die Registerkarte ERWEITERT

Wichtig

Die verschiedenen Einstellungsmöglichkeiten des Applets INTERNETOPTIONEN sollten Sie kennen.

Hinweis

In der Systemsteuerung von Windows gibt es ein Applet namens ANMELDEINFORMATIONSVERWALTUNG, mit dem Sie die gespeicherten Zugangsdaten für Websites, verbundene Anwendungen und Netzwerke verwalten können. Hier können Sie Kennwörter oder andere Zugangsdaten löschen.

Andere Webbrowser konfigurieren

Ich würde jetzt gerne auf dem Internet Explorer herumtrampeln und Ihnen erklären, wie schlecht er ist. Tatsache ist jedoch, dass Microsoft nach vielen vergeblichen Anstrengungen in den letzten Versionen, den Internet Explorer endlich in den Griff zu bekommen, das Richtige getan hat und ihn nicht weiterentwickelt. Stattdessen konzentriert man sich auf den Nachfolger Microsoft Edge. Edge ist ein leistungsfähiger, sauber programmierter moderner Webbrowser, der die aktuellen Webstandards unterstützt. Ich verwende ihn häufig, wenn auch nicht ausschließlich.

Sie möchten sich vermutlich einen der anderen Browser herunterladen, die aktuelle Standards ebenfalls unterstützen und eine andere Erfahrung als Edge bieten. Sie verfügen dann über Ausweichmöglichkeiten, wenn eine Website Schwierigkeiten bereitet oder eine gefährliche Sicherheitslücke in Ihrem üblichen Browser entdeckt wird. Die beiden Schwergewichte in dieser Kategorie sind Mozilla Firefox und Google Chrome.

Die Konfiguration geschieht im Prinzip auf die gleiche Art und Weise wie beim Internet Explorer, allerdings werden Sie dafür kein Applet in der Systemsteuerung finden. Klicken Sie in Google Chrome auf das Symbol (drei Punkte) in der oberen rechten Ecke und wählen Sie EINSTELLUNGEN aus. In Mozilla Firefox sieht das Symbol ähnlich aus (drei Linien), es befindet sich jedoch an der gleichen Stelle und der Menüpunkt heißt ebenfalls EINSTELLUNGEN.

In diesen Menüs werden Sie eine Menge Einstellungen finden, die denen des Internet Explorers sehr ähnlich sind. Die Einstellungen in Firefox (Abbildung 21.30) und Google Chrome (Abbildung 21.31) sind in den Browser integrierte Webseiten, steuern aber ebenfalls dieselben Funktionen: Startseite, Sicherheit, Schriftart und -größe, Cookies und natürlich Ihre Favoriten. Nehmen Sie sich etwas Zeit, um diese Browser auszuprobieren und deren Einstellungen zu erforschen. Sie werden erstaunt sein, wie sehr Ihnen das Wissen über einen Browser beim Einrichten eines anderen zugutekommt.

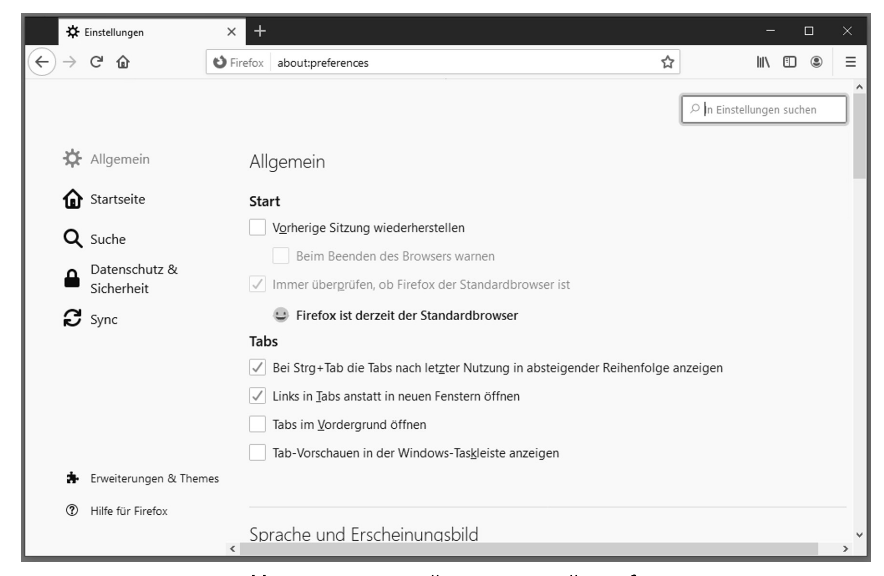


Abb. 21.30: Die Einstellungen in Mozilla Firefox

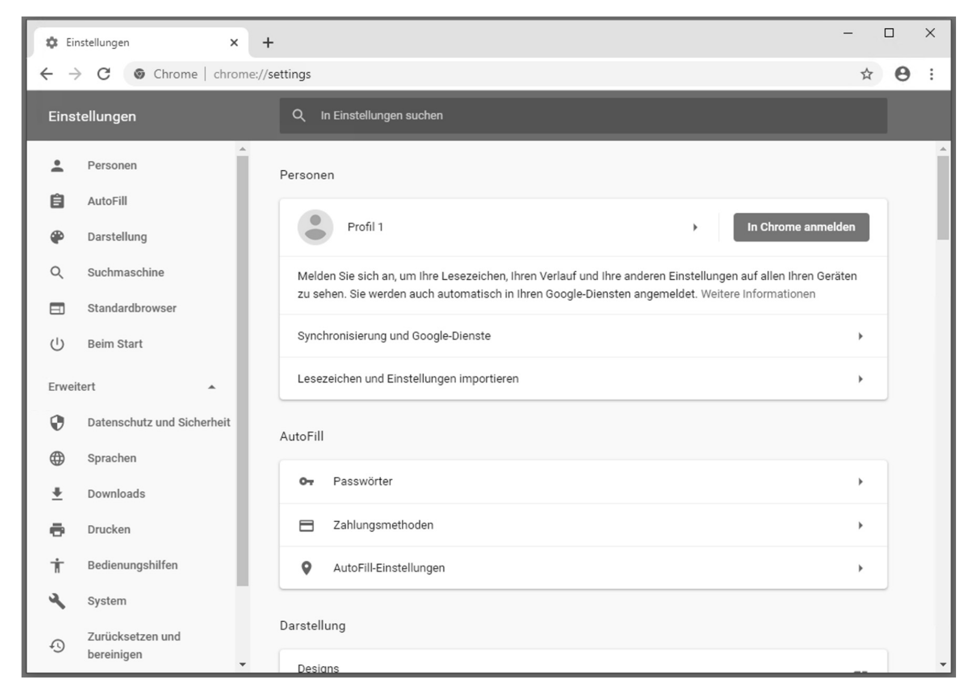


Abb. 21.31: Die Einstellungen in Google Chrome

Hinweis

Wenn Sie einen macOS-Computer verwenden, werden Sie wahrscheinlich einen anderen Browser verwenden, nämlich Safari. Safari unterstützt alle modernen Webstandards und funktioniert bestens. Chrome, Firefox und neuerdings auch Edge sind ebenfalls für macOS verfügbar. Viel Spaß beim Surfen!

21.3.2 E-Mail

Für den Versand und Empfang von *E-Mail* stehen Ihnen heutzutage viele Optionen zur Verfügung. Natürlich können Sie die herkömmliche Methode verwenden, die ein eigenständiges E-Mail-Programm erfordert. Zunehmend werden jedoch E-Mail-Clients genutzt, die fest in die Geräte integriert sind. Und dann gibt es ja auch noch webbasierte E-Mail-Clients, die von jedem Gerät aus zugänglich sind. Ein wenig problematisch ist an dieser Stelle, dass immer mehr Leute sich mit Benutzerkonten von Internetdiensten an ihren Geräten anmelden, z.B. wenn man sein Microsoft-Benutzerkonto verwendet, um sich am Windows-PC einzuloggen.

E-Mail-Adressen werden im heute weithin bekannten Format `Kontoname@Internetdomäne` formuliert. Zum Hinzufügen eines neuen Benutzerkontos müssen Sie Name, E-Mail-Adresse und Kennwort angeben. Das ist schon alles, was Sie tun müssen, sofern der Server richtig konfiguriert ist.

Es ist noch gar nicht so lange her, dass es eine ziemliche Herausforderung darstellte, einen E-Mail-Client einzurichten (in den CompTIA-Prüfungen wird noch immer darauf verwiesen). Sie musten nicht nur eine gültige E-Mail-Adresse und ein Kennwort vom ISP erhalten, sondern auch die Informationen über die Server für ein- und ausgehende Nachrichten konfigurieren. Sie mussten die Namen des POP3- (*PostOffice Protocol version 3*) oder IMAP4- (*Internet Message Access Protocol 4*) und des SMTP-Servers (*Simple Mail Transfer Protocol*) angeben. Der POP3- bzw. IMAP-Server ist der Computer, der eintreffende E-Mail für Sie entgegennimmt. Der am weitesten verbreitete Standard ist die neueste IMAP-Version, IMAP4. Der SMTP-Server erledigt den Versand ausgehender E-Mails.

Wichtig

Sie sollten die Portnummern dieser E-Mail-Protokolle kennen! POP3 verwendet Port 110, IMAP4 verwendet Port 143 und SMTP nutzt Port 25. In der Prüfung kommen fast mit Sicherheit Fragen vor, bei denen es darum geht, welche Protokolle für eingehende (POP3 und IMAP4) und ausgehende (SMTP) Mail zuständig sind.

Integrierte E-Mail-Programme

Alle mobilen Geräte verfügen über einen integrierten E-Mail-Client, der für die meisten mobilen Mailumgebungen vorkonfiguriert ist. Auf Geräten von Apple, wie dem iPad, können Sie sich ein iCloud-Benutzerkonto einrichten und all Ihre iCloud-fähigen Geräte miteinander synchronisieren. Bei der Einrichtung eines E-Mail-Kontos brauchen Sie nichts weiter zu konfigurieren, weil vorausgesetzt wird, dass der Versand und der Empfang von E-Mails über iCloud erfolgen. Die Konfiguration von IMAP, POP, SMTP usw. findet hinter den Kulissen statt. Die CompTIA bezeichnete diese Art der automatischen Konfiguration als *integrierte E-Mail-Konfiguration durch kommerzielle Anbieter*. Das klingt zwar langweilig, trifft den Nagel aber auf den Kopf. Mehr darüber erfahren Sie im Kapitel 24, *Mobile Geräte*.

Webmail

Viele Leute verwenden *Webmailer* wie Yahoo! Mail, Gmail von Google oder Exchange Online von Microsoft zur Abwicklung ihres E-Mail-Verkehrs (Abbildung 21.32). Webmailer besitzen den Vorteil, dass sie von jedem mit dem Internet verbundenen Gerät aus zugänglich sind, sei es nun ein Computer, ein Smartphone oder ein Tablet.

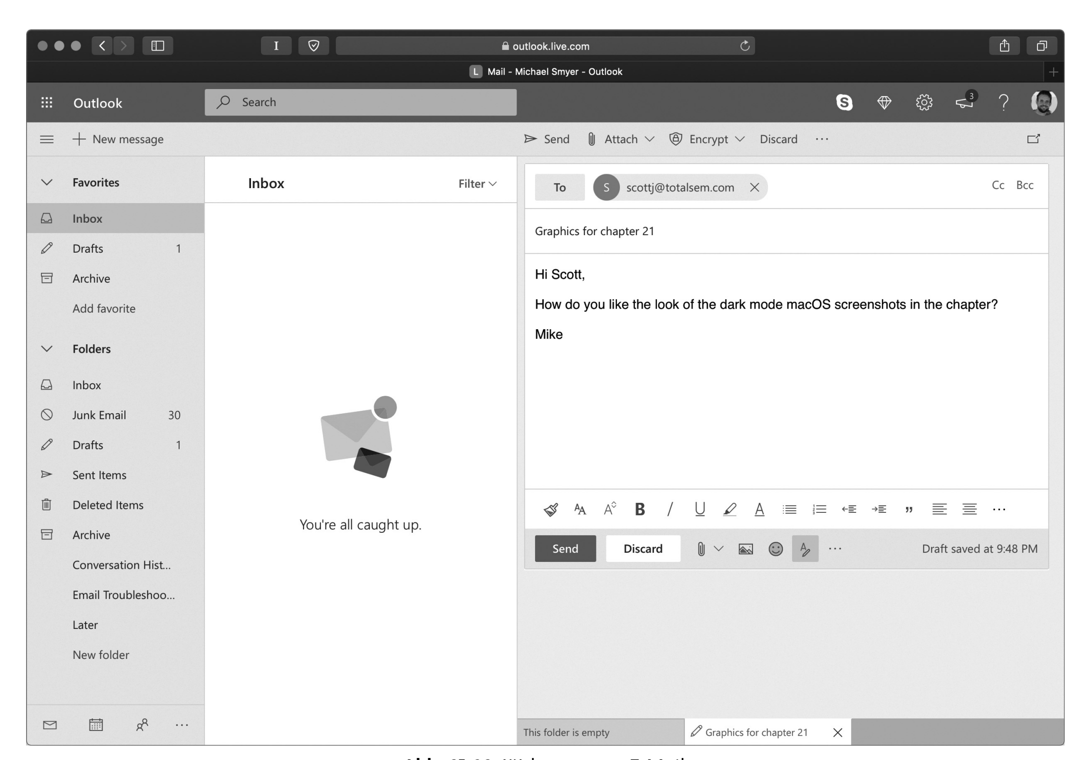


Abb. 21.32: Webgestützte E-Mail

Die Vorzüge eigenständiger E-Mail-Programme sind vor allem die besseren Möglichkeiten, E-Mails zu verwalten, zu markieren, zu durchsuchen usw. Allerdings haben die Webmailer in vielerlei Hinsicht aufgeholt. Beispielsweise bieten Webdienste erheblich bessere Spamfilter, weil sie auf das Feedback einer sehr großen Benutzergemeinde zurückgreifen können, die vor unerwünschten oder gefährlichen E-Mails warnt.

Vereinheitlichte Benutzerkonten

Wenn ich mich an meinem Rechner mit Windows 10 anmelde, verwende ich dazu mein Microsoft-Benutzerkonto, ein vollwertiges E-Mail-Konto, das sich auf den Servern von Outlook befindet. Auf diese Weise ist mein Rechner in der Lage, sich mit dem Mailserver zu verbinden. Wenn ich den E-Mail-Client öffne, kann ich unmittelbar auf mein Hotmail-Konto zugreifen (Abbildung 21.33). Für den Benutzer oder einen Techniker gibt es hier nichts zu konfigurieren. Gleiches gilt für die Geräte von Apple, sei es nun ein mobiles Gerät, wie ein Smartphone, oder ein Desktop-Rechner, auf dem macOS läuft. Microsoft nennt diese Funktionalität *Live-Anmeldung*.

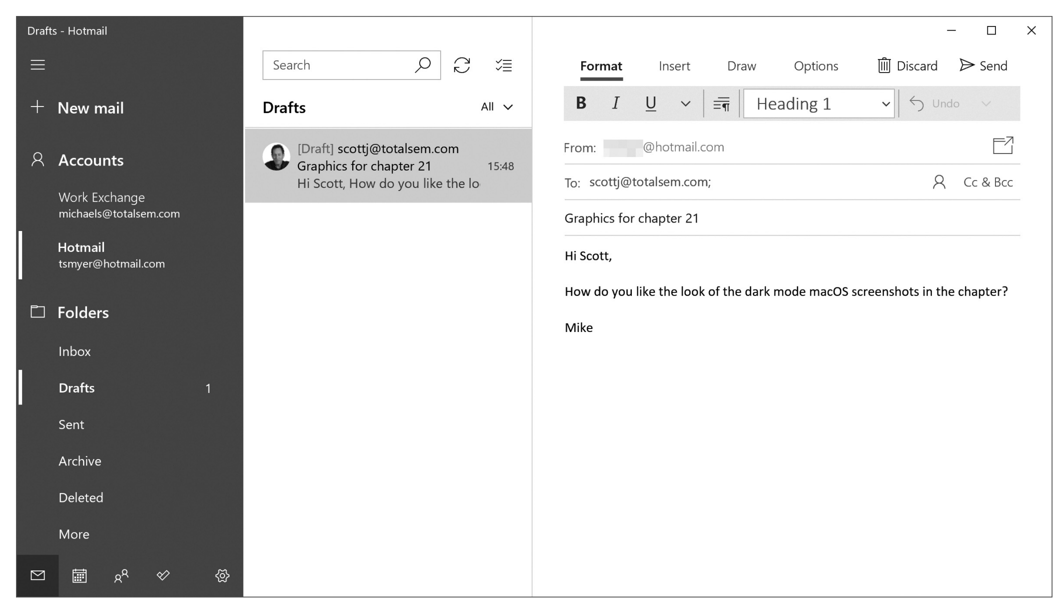


Abb. 21.33: Mail in Windows 10

21.3.3 FTP (File Transport Protocol)

FTP (*File Transfer Protocol*) verwendet die Ports 20 und 21 und eignet sich hervorragend für den Austausch von Dateien zwischen Systemen. FTP-Serversoftware gibt es für die meisten Betriebssysteme, sodass sich Dateien unabhängig vom Betriebssystem zwischen zwei Systemen übertragen lassen. Zum Zugriff auf eine FTP-Site müssen Sie einen FTP-Client wie etwa *FileZilla* verwenden, auch wenn die meisten Webbrowser zumindest FTP-Downloads auch direkt unterstützen. Sie geben einfach den Namen der FTP-Site in die Adressleiste ein. Abbildung 21.34 zeigt Mozilla Firefox beim Zugriff auf `ftp://ftp.kernel.org`.

Obwohl Sie auch mit einem Webbrowser arbeiten können, müssen Sie sich bei allen FTP-Sites anmelden. Ihr Webbrowser wird dabei versuchen, Sie mit dem Benutzernamen »anonymous« und leerem Kennwort anzumelden. Wenn Sie sich als ein bestimmter Benutzer anmelden wollen, müssen Sie Ihren Benutzernamen zur URL hinzufügen. (Statt beispielsweise `ftp://ftp.beispiel.com` einzutragen, würden Sie `ftp://benutzername@ftp.beispiel.com` eingeben.) Bei fast allen öffentlichen

FTP-Sites kann man sich auch anonym anmelden. Viele Techniker bevorzugen für den FTP-Zugriff Programme von Drittanbietern, wie etwa FileZilla oder *Cyberduck* für macOS (Abbildung 21.35), weil diese Programme den Benutzernamen und die Kennworteinstellungen speichern. Auf diese Weise können Sie später einfacher wieder auf die FTP-Site zugreifen. Beachten Sie, dass FTP in einer vertrauensseligeren Zeit entwickelt wurde und dass Benutzername und Kennwort unverschlüsselt und im Klartext über das Netzwerk übertragen werden. Sie sollten für eine FTP-Site daher keinesfalls dasselbe Kennwort verwenden wie für Ihre Domänenanmeldung im Büro!

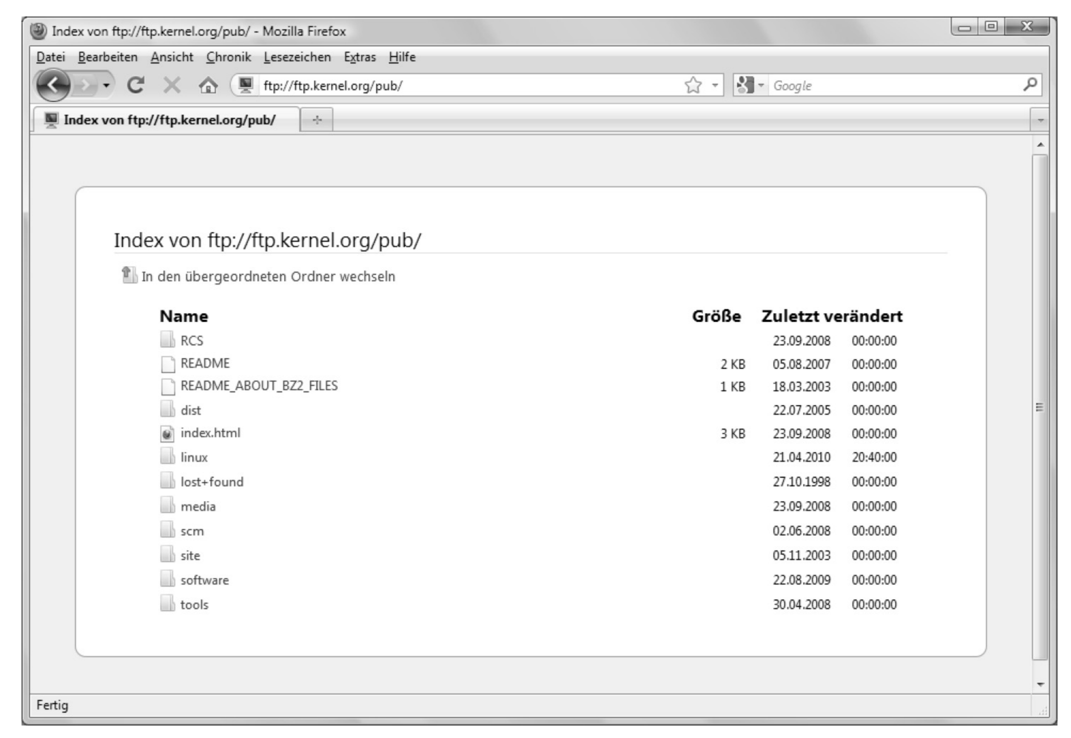


Abb. 21.34: Zugriff auf einen FTP-Server mit Firefox

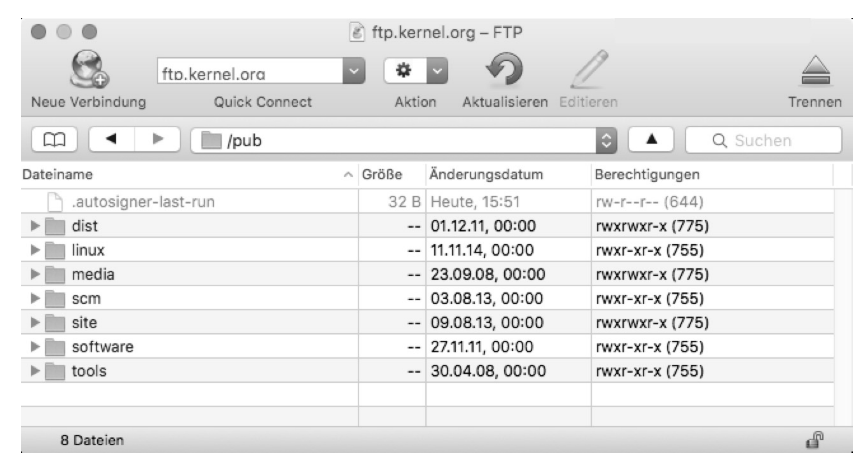


Abb. 21.35: Das FTP-Programm Cyberduck für macOS

21.3.4 Telnet und SSH

Telnet ist ein Terminalemulationsprogramm für TCP/IP-Netzwerke, das Sie mit einem Server oder einem Router auf Port 23 verbindet und Befehle auf dem Gerät so ausführt, als säßen Sie direkt davor. Auf diese Weise können Sie aus der Ferne einen Server verwalten und mit anderen Servern im Netzwerk kommunizieren. Wie Sie sich vorstellen können, ist dies ziemlich riskant. Wenn *Sie* einen Computer aus der Ferne steuern können, was hindert dann andere Leute daran, es Ihnen gleichzutun? Natürlich erlaubt Telnet nicht jedermann die Anmeldung und absichtliche Manipulation Ihres Netzwerks. Sie müssen einen bestimmten Benutzernamen und ein Kennwort eingeben, um Telnet nutzen zu können. Leider besitzt Telnet dieselben schlechten Angewohnheiten wie FTP und sendet Kennwörter und Benutzernamen im Klartext, deshalb sollten Sie es grundsätzlich nur innerhalb Ihres eigenen LANs benutzen.

Wenn Sie ein entferntes Terminal benötigen, das sicher über das Internet funktioniert, sollten Sie *SSH* (*Secure Shell*) benutzen. Tatsächlich hat SSH heute Telnet in fast allen Bereichen verdrängt, in denen es dereinst beliebt war. Für den Anwender funktioniert SSH genau wie Telnet. Im Hintergrund verwendet SSH Port 22 und arbeitet mit vollständig verschlüsselten Verbindungen, die dafür sorgen, dass kein Lauscher Ihre Daten abhört. SSH hat noch einen weiteren Trumpf im Ärmel und kann Dateien oder beliebigen TCP/IP-Netzwerkverkehr über seine sichere Verbindung übertragen. Im Netzwerkjargon nennt man das *Tunneling* und dabei handelt es sich um den Kern von Technologien wie SFTP und VPN, auf die ich in diesem Kapitel noch genauer eingehen werde.

Wichtig

Für die CompTIA A+-Prüfung 1002 müssen Sie einige Netzwerktools (wie z.B. Telnet) kennen, aber nur insoweit, um einen Netzwerktechniker oder einen Administrator unterstützen zu können. Wenn Sie Telnet oder SSH benutzen müssen, wird man Ihnen die Details nennen. Die Implementierungen von Telnet und SSH gehen weit über den Rahmen der CompTIA A+-Prüfung hinaus.

21.3.5 SFTP

Sicheres FTP ist nichts weiter als normales FTP, das über einen verschlüsselten SSH-Tunnel geleitet wird. Sie können (und sollten!) SFTP für die gleichen Aufgaben verwenden, für die Sie sonst FTP benutzen würden, es ist jedoch technisch gesehen ein eigenes Protokoll. Das SFTP-Protokoll ist eine Erweiterung von SSH, deshalb gibt es SSH-Software, die SFTP-Client und SFTP-Server unterstützt, wie das verbreitete *OpenSSH*, ein beliebter SSH-Server, der auch SFTP-Funktionen mitbringt. In Abbildung 21.36 verwende ich SFTP, um das Protokoll eines Webservers zu übertragen.

```
mikesmyer — ssh ◂ sftp totalcom@totalsem.com — 5...
sftp> get totalsem.com-Oct-2018.gz
Fetching /home/totalcom/logs/totalsem.com-Oct-2018.gz to
totalsem.com-Oct-2018.gz
/home/totalcom/logs/to 100% 7621KB   3.2MB/s   00:02
sftp> █
```

Abb. 21.36: OpenSSH

21.3.6 VoIP (Voice over IP)

Voice over IP (*VoIP*) ermöglicht Ihnen, ganz normale Telefongespräche über Ihr Computernetzwerk zu führen. Warum brauchen Sie zwei Leitungen, eine für Sprache, eine für Daten, an jedem Schreibtisch? Warum nutzen Sie nicht einfach die überflüssige Kapazität des Datennetzwerks für Ihre Telefonanrufe? Genau das erledigt VoIP für Sie. VoIP lässt sich mit jeder Art schneller Internetverbindung nutzen, also über DSL, Kabel und Satellit.

VoIP bezieht sich nicht auf ein einzelnes Protokoll, sondern vielmehr auf eine ganze Sammlung von Protokollen, die Telefongespräche über Datennetzwerke ermöglichen. Das am weitesten verbreitete Protokoll heißt *SIP* (*Session Initiation Protocol*), aber einige der beliebtesten VoIP-Applikationen wie Skype verwenden ausschließlich proprietäre Protokolle.

Anbieter wie etwa Skype, Cisco, Vonage, Arris oder Comcast liefern beliebte VoIP-Lösungen, und viele Unternehmen verwenden VoIP für ihre internen Telefonnetzwerke. Bei der Installation und Problembehebung im VoIP-Bereich sollten Sie sich unbedingt merken, dass hier niedrige Latenzzeiten wichtiger als hohe Netzwerkgeschwindigkeiten sind. Die *Latenz* gibt die Zeitspanne an, die ein Paket benötigt, um seinen Zielort zu erreichen, und bemisst sich in Millisekunden. Je höher die Latenz, desto größer werden die durch spürbare Verzögerungen in VoIP-Telefonaten verursachten Irritationen und damit auch die Probleme.

VoIP ist aber nicht nur per Computer nutzbar, sondern kann eine Telefonanlage mit Kupferkabeln vollständig ersetzen. Bei der Einrichtung eines VoIP-Systems gibt es zwei beliebte Methoden: Man kann eigenständige VoIP-Telefone verwenden, wie sie beispielsweise Cisco herstellt, oder die vorhandenen, analogen Telefone an VoIP-Telefonadapter (Abbildung 21.37) anschließen.

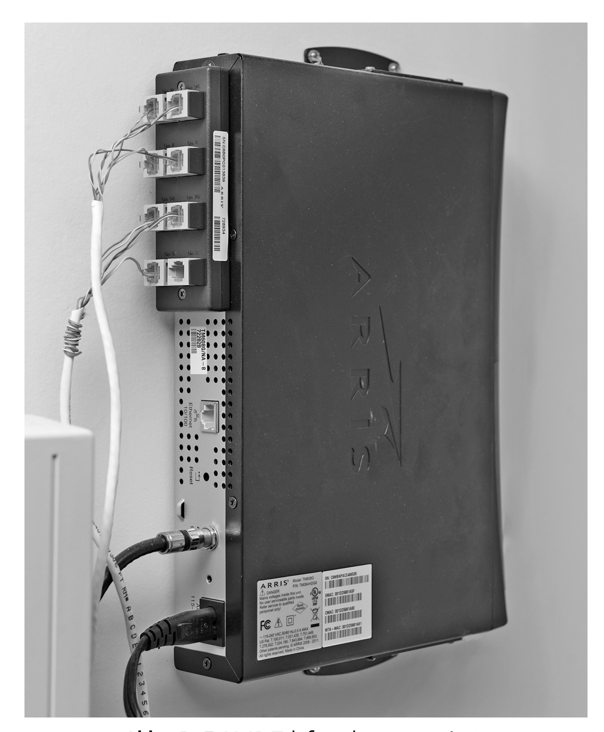


Abb. 21.37: VoIP-Telefonadapter von Arris

Echte VoIP-Telefone besitzen einen RJ-45-Anschluss, der direkt mit dem Netzwerk verbunden wird, und bieten Funktionen wie qualitativ hochwertige Audio- und Videoübertragungen. Leider sind zum Betrieb solcher Telefone komplexe, kostspielige Netzwerke erforderlich und dadurch werden sie für die meisten Haushalte uninteressant.

In Privathaushalten sind eher VoIP-Telefonadapter zum Anschluss analoger Telefone gebräuchlich. Diese kleinen Kästchen werden einfach ans Netzwerk angeschlossen und schon können Sie ein (analoges) Telefon anschließen und prüfen, ob Sie ein Freizeichen hören. Bei den von Kabelnetzbetreibern angebotenen Diensten ist der Adapter oft in das Kabelmodem integriert, was den Anschluss eines Telefons zum Kinderspiel macht.

Tipp

Aufgrund all der Probleme, die sie verursachen, sind zu hohe Latenzzeiten die Geißel der VoIP-Telefonie. Eine einfache Möglichkeit, die aktuelle Latenz zu messen, bietet das immer wieder praktische `ping`. Probieren Sie Folgendes:

1. Pingen Sie einen wohlbekannten Server wie `www.microsoft.com` oder `www.totalsem.com` an.
2. Vor dem Beenden gibt `ping` eine Statistik aus. Die als »Mittelwert« bezeichnete Zeitangabe ist Ihre aktuelle Latenzzeit.

21.3.7 Remotedesktop

In Netzwerken geben wir hauptsächlich Ordner und Drucker frei. Manchmal wäre es jedoch praktisch, vor einem anderen Computer zu sitzen – und zwar so, als hätte man wirklich seine Tastatur zur Verfügung. Es gibt eine Reihe von Programmen zur Fernsteuerung, die genau das ermöglichen und als *Remotedesktop* bezeichnet werden.

Hinweis

Da *Remotedesktop* ein allgemeiner Begriff ist, gibt es einige Programme mit irritierend ähnlichen Namen. So hatten sowohl Microsoft als auch Apple zeitweilig ein Programm namens »Remotedesktop« im Angebot. (Letzteres ist kostenpflichtig). Allerdings nennt Microsoft das Programm in neueren Windows-Versionen »Remotedesktopverbindung«. Und dann gibt es auch noch Microsoft Remote Desktop für macOS, mit dem Macs Windows-Rechner fernsteuern können.

Manche Betriebssysteme bringen von Haus aus einen Remotedesktopclient mit, dennoch gibt es eine Reihe von Remotedesktopprogrammen von Drittanbietern. Die meisten nutzen entweder *RDP* (*Remote Desktop Protocol*) oder *VNC* (*Virtual Network Computing*). *TightVNC* beispielsweise ist kostenlos und plattformübergreifend, sodass Sie beispielsweise ein Windows-System entfernt von Ihrem Macintosh aus steuern können – oder umgekehrt. Abbildung 21.38 zeigt VNC bei der Arbeit.

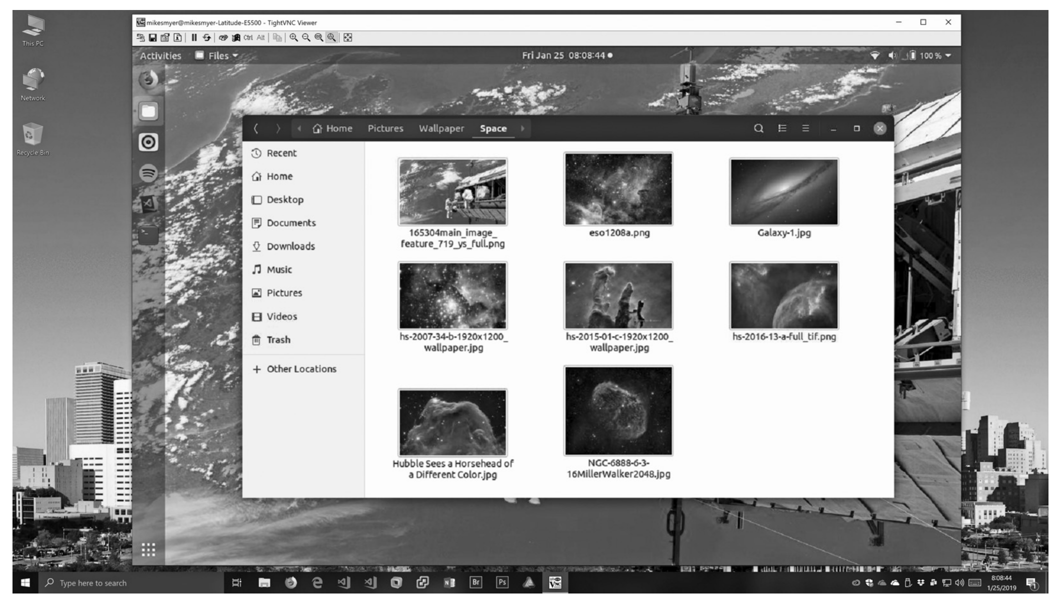


Abb. 21.38: VNC in Aktion

Hinweis

Zur Fernsteuerung sind separate Server- und Client-Programme erforderlich.

Die heutigen Windows-Versionen bieten eine Alternative zu VNC: *Remotedesktopverbindung*. Es erlaubt die Kontrolle über einen entfernten Server mit der vollständigen grafischen Benutzeroberfläche. Ihr Desktop *wird* zum Server-Desktop (Abbildung 21.39).

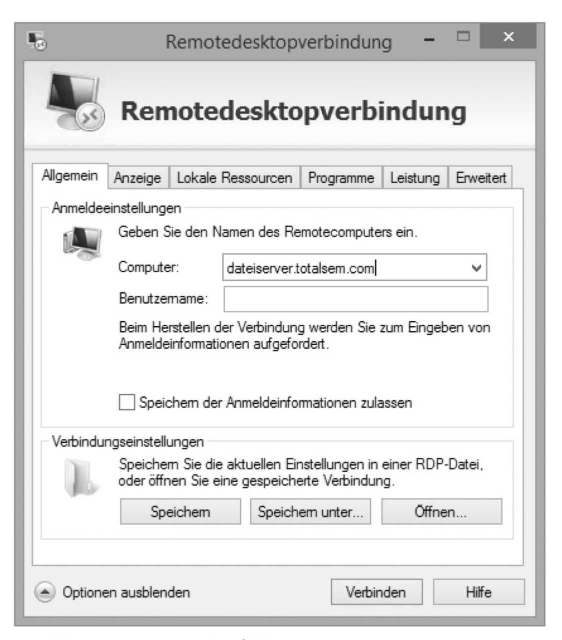


Abb. 21.39: Das Dialogfeld REMOTEDESKTOPVERBINDUNG

Hinweis

Die ausführbare Datei der Remotedesktopverbindung heißt `mstsc.exe`. Sie können das Programm von der Eingabeaufforderung oder dem Suchfeld aus starten, indem Sie `mstsc` eingeben und ↵ drücken.

Wäre es nicht praktisch, wenn Sie bei einer technischen Anfrage einfach sehen könnten, was Ihr Kunde sieht? Wenn der Kunde sagt, dass irgendetwas nicht funktioniert, dann wäre es doch wunderbar, wenn Sie von Ihrem Schreibtisch zum Schreibtisch Ihres Kunden wechseln könnten, um genau zu sehen, was er meint. Das würde die Missverständnisse wesentlich reduzieren, die dem Techniker das Leben so schwer machen. *Windows-Remoteunterstützung* hilft Ihnen dabei. Es erlaubt Ihnen, jedem die Kontrolle über Ihren Desktop zu überlassen. Wenn ein Benutzer ein Problem hat, kann er den Support direkt von Ihnen anfordern. Nachdem Sie die Support-Anfrage per E-Mail erhalten haben, melden Sie sich an seinem System an und übernehmen mit seiner Erlaubnis die Kontrolle. Abbildung 21.40 zeigt die Remoteunterstützung in Aktion.

Mit der Remoteunterstützung können Sie alles machen, was Sie auch direkt am jeweiligen Computer tun könnten. Sie können Hardwarekonfigurationen überprüfen oder Treiberprobleme lösen. Sie können Treiber installieren, Treiber zurücksetzen, neue Treiber herunterladen usw. Sie steuern die entfernte Maschine, solange der Kunde Ihnen das erlaubt. Der Kunde sieht alles, was Sie machen, und kann Sie sofort unterbrechen, wenn Sie irgendetwas tun, das ihn nervös macht. Remoteunterstützung

kann Ihnen helfen, jemandem zu zeigen, wie ein bestimmtes Programm funktioniert. Sie melden sich auf dem PC eines Benutzers an, starten Outlook oder Mail und durchlaufen dann die Konfigurationsschritte, während der Benutzer zusieht. Der Benutzer kann dann seinen Computer wieder übernehmen und die Schritte selbst nachvollziehen, während Sie zusehen, und dabei die ganze Zeit über mit Ihnen sprechen. Großartig!



Abb. 21.40: Windows-Remoteunterstützung

Wichtig

Apple bietet für Unternehmenskunden ein Remotedesktopprodukt an, dass ebenfalls Remoteunterstützung mitbringt. Oft ist das aber gar nicht nötig, denn zu macOS gehört auch ein etwas einfacheres Werkzeug namens *Bildschirmfreigabe*. Diese zum Betriebssystem gehörende Funktionalität kann in den Systemeinstellungen unter FREIGABEN aktiviert werden. Das Programm BILDSCHIRMFREIGABE zur Steuerung finden Sie unter `/System/Library/CoreServices/Applications`. Zum Fernsteuern, zum Datenaustausch und für die gelegentliche Fehlerbehebung aus der Ferne ist die Bildschirmfreigabe mehr als ausreichend.

Die grafischen Fernsteuerungsprogramme bieten alles, was Sie brauchen, um von einem System aus auf ein anderes zuzugreifen. Sie sind sehr gebräuchlich, insbesondere seitdem Microsoft diese kostenlos bereitstellt. Egal, welches Programm Sie verwenden, Sie benötigen immer sowohl ein Server- als auch ein Client-Programm. Der Server muss auf dem System installiert werden, auf das Sie zugreifen wollen, und der Client auf dem System, das Sie zur Fernsteuerung verwenden. Bei vielen der Fernsteuerungsprogramme sind Server und Client in ein einziges Produkt integriert.

Sie können die Remoteunterstützung in Windows aktivieren und deaktivieren sowie andere Einstellungen vornehmen. Öffnen Sie in der Systemsteuerung das Applet SYSTEM und klicken Sie auf REMOTEINSTELLUNGEN. Auf der Registerkarte REMOTE finden Sie Kontrollkästchen zur Aktivierung von Remoteunterstützung und Remotedesktop sowie Schaltflächen zur Konfiguration erweiterter Einstellungen.

Wichtig

In Windows können Sie bestimmte Anwendungen ausführen, die von einem anderen Windows-Rechner gehostet werden. Stellen Sie sich das Ganze wie eine Remotedesktopverbindung ohne Desktop vor. Die

Anwendung läuft auf einem Computer, dem Server, wird aber auf einem anderen Computer, dem Client, dargestellt und bedient. Sie können eine solche Verbindung mit einem Server in der Systemsteuerung über REMOTEAPP UND DESKTOPVERBINDUNGEN einrichten.

21.3.8 VPN (Virtuelles privates Netzwerk)

Remoteverbindungen gibt es bereits seit langer Zeit, länger noch als das Internet. Der größte Nachteil von Remoteverbindungen bestand in ihren Verbindungskosten. Wenn Sie sich an einem Ende eines Kontinents oder eines Landes befanden und sich mit Ihrem LAN am anderen Ende des Kontinents oder Landes verbinden mussten, dann stand nur das Telefon als Verbindungsoption zur Verfügung. Oder Sie mussten, wenn Sie zwei LANs über weite Entfernungen miteinander verbinden wollten, horrende monatliche Gebühren für eine private Verbindung bezahlen. Mit der Einführung des Internets entstand für Menschen, die sich mit ihren Heimnetzwerken verbinden wollten, eine sehr preiswerte Verbindungsoption, die aber ein Problem mit sich brachte, da das gesamte Internet öffentlich zugänglich ist. Man wollte zwar keine Wählverbindungen oder teure private Verbindungen mehr verwenden und hätte lieber das Internet benutzt, aber das sollte auch sicher sein.

Die schlauen Netzwerkentwickler arbeiteten lang und hart und stellten dann mehrere Lösungen für dieses Problem vor. Es wurden Standards entwickelt, die verschlüsselte Tunnel zwischen Computern (oder Netzwerken an entfernt gelegenen Standorten) benutzten, um private Netzwerke über das Internet aufzubauen (Abbildung 21.41). Das Ergebnis ist unter dem Namen *VPN* (*Virtual Private Network*) bekannt.

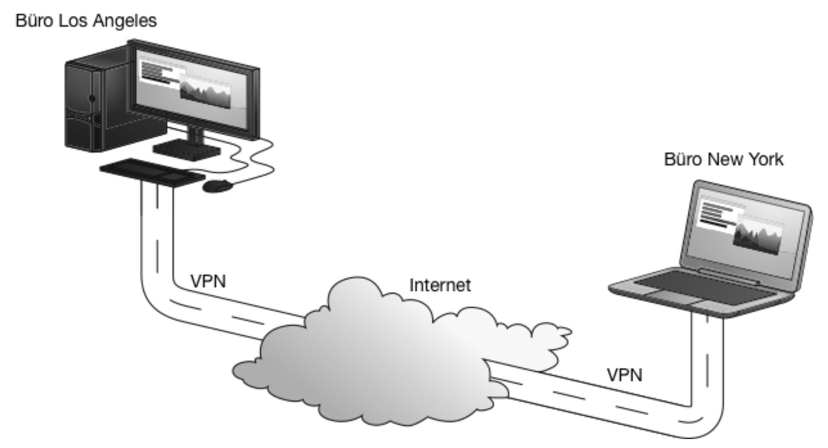


Abb. 21.41: Ein VPN verbindet Computer über die Vereinigten Staaten hinweg.

Ein verschlüsselter Tunnel erfordert Endpunkte, an denen die Daten verschlüsselt und entschlüsselt werden. Beim bereits vorgestellten SSH-Tunnel befinden sich der Client der Anwendung am einen und der Server am anderen Ende. Das ist auch bei VPNs so. Irgendwelche auf einem Rechner ausgeführten Programme oder manchmal auch eigens dafür vorgesehene Geräte müssen als Endpunkte eines VPNs fungieren (Abbildung 21.42).

Damit VPNs funktionieren, wird ein Protokoll benötigt, das eines der vielen verfügbaren Tunneling-Protokolle nutzt und zudem eine IP-Adresse von einem lokalen DHCP-Server anfordern kann, um dem Tunnel eine IP-Adresse zuweisen zu können, die zum Subnetz des lokalen LANs gehört. Die Verbindung behält ihre IP-Adresse für die Internetverbindung, aber die Tunnelendpunkte müssen sich wie Netzwerkadapter verhalten (Abbildung 21.43). Sehen wir uns nun eines dieser Protokolle namens PPTP an.

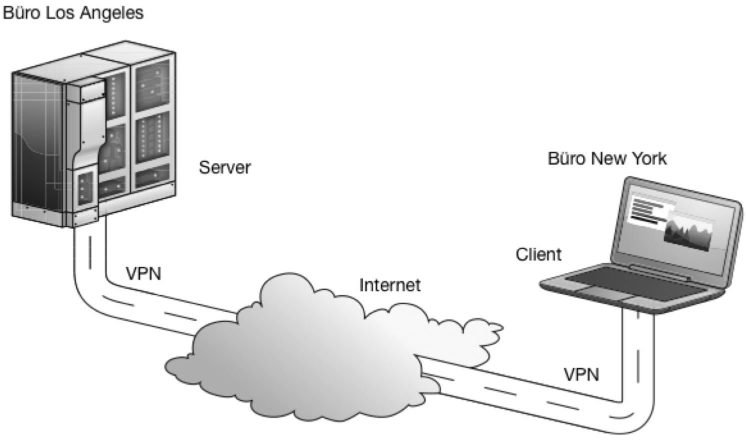


Abb. 21.42: Ein typischer VPN-Tunnel

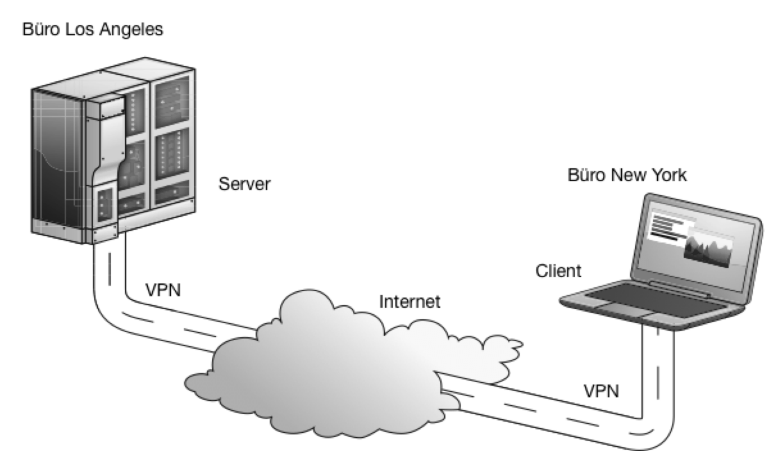


Abb. 21.43: Die Endpunkte müssen ihre eigenen IP-Adressen besitzen.

PPTP-VPNS

Wie können wir IP-Adressen aus dem Nichts erscheinen lassen? Microsoft gab mit *PPTP* (*Point-to-Point Tunneling Protocol*) den Anstoß. Bei diesem Protokoll handelt es sich um eine weiterentwickelte Version des bereits erwähnten Protokolls PPP, das für Wählverbindungen ins Internet verwendet wurde und das bereits von Beginn an all das beherrschte. Der einzige Trick betrifft die Endpunkte. Aus der Sicht von Microsoft sollen VPNs für die Verbindung einzelner Clients (denken Sie an reisende Angestellte) mit ihrem Büronetzwerk sorgen. Daher platzierte Microsoft die PPTP-Endpunkte beim Client und ein spezielles Remotezugriff-Serverprogramm namens *RRAS* (*Routing and Remote Access Service*), das ursprünglich nur unter Windows Server zur Verfügung stand, auf dem Server (Abbildung 21.44).

Aufseiten des Windows-Clients geben Sie unter Windows 7 ins Suchfeld `VPN` ein und drücken [↵]. Unter Windows 8/8.1/10 tippen Sie auf dem Startbildschirm `VPN` ein, wählen aus den Suchtreffern VIRTUELLE PRIVATE NETZWERKE (VPNS) VERWALTEN (Windows 8/8.1) oder VPN EINSTELLUNGEN (Windows 10) aus und klicken auf VPN-VERBINDUNG HINZUFÜGEN. Daraufhin werden Dialogfelder angezeigt, in denen Sie die Daten Ihres VPN-Servers eintragen können. Ihr Netzwerkadministrator

sollte Ihnen die dabei benötigten Informationen geben. Das Ergebnis ist eine virtuelle Netzwerkkarte, der wie allen anderen auch eine IP-Adresse vom DHCP-Server in Ihrem Büro zugewiesen wird (Abbildung 21.45).

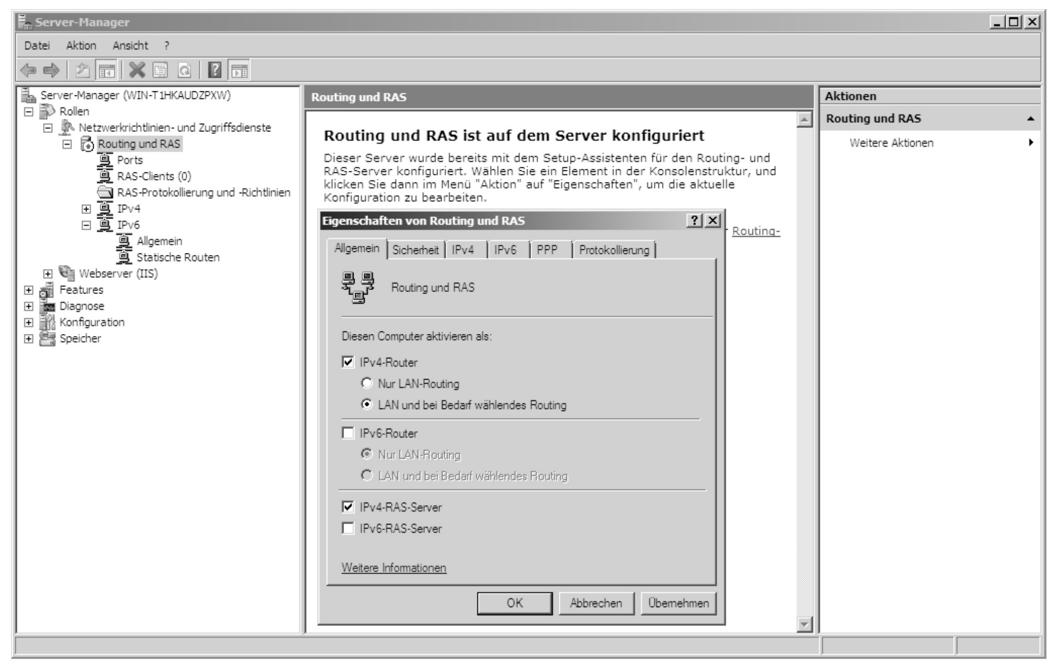


Abb. 21.44: RRAS in Aktion



Abb. 21.45: Eine VPN-Verbindung unter Windows

Wichtig

Ein mit dem VPN verbundenes System verhält sich, als befände es sich im lokalen Netzwerk, arbeitet aber oft viel langsamer als ein im Büro direkt mit dem LAN verbundener Rechner.

Wenn sich Ihr Computer mit dem RRAS-Server im privaten Netzwerk verbindet, dann erzeugt PPTP einen sicheren Tunnel durch das Internet zurück ins private LAN. Ihr Client erhält eine IP-Adresse dieses Netzwerks, so als wäre der Rechner an das LAN im Büro angeschlossen. Selbst Ihr Internetverkehr geht erst über Ihr Büro. Wenn Sie Ihren Webbrowser starten, dann nimmt Ihr Client den Weg über das Internet zum Büro-LAN und benutzt dann dessen Internetverbindung! Deswegen surft man über ein VPN nur sehr langsam im Web.

21.3.9 File Sharing

Der letzte Internetdienst, den wir hier betrachten, dürfte auch der umstrittenste sein: *File Sharing*. File Sharing entwickelte sich Ende der 1990er-Jahre. Dabei läuft auf vielen Computern das gleiche Programm, wie etwa Napster oder Kazaa. Das File-Sharing-Programm ermöglicht es den Computern, Dateien wie Musik oder Spielfilme anzubieten. Wenn alle File-Sharing-Programme mit dem Internet verbunden sind, kann jedes davon auf die von den anderen angebotenen Dateien zugreifen und sie herunterladen.

Beim File Sharing durch *verteilte* Sharing-Software hat man den Eindruck, anonym zu bleiben und dass alles kostenlos ist – das ist das Problem. Man kann *alles* mit anderen teilen, auch urheberrechtlich geschützte Spielfilme, Musik und dergleichen mehr. Die Musikbranche und später auch die Filmbranche haben versucht, File Sharing zu unterbinden. Das hatte eine Reihe von Gerichtsverfahren gegen Unternehmen zur Folge, die das File Sharing erleichterten, und gegen Einzelpersonen, die sehr viele Dateien anboten.

Wichtig

Rechnen Sie in der CompTIA A+-Prüfung 1001 mit Fragen zum Thema *File-Share-Technologien*. Normalerweise wird zwar immer der Begriff *File Sharing* verwendet, gemeint ist jedoch dasselbe: die Verwendung legaler Technologien zum Zugriff auf legale und illegale Inhalte.

Softwareentwickler und File Sharer gaben aber nicht nach und reagierten auf den Druck durch die Erfindung von Internetprotokollen wie *Bit Torrent*, mit dem sich Dateien schneller und effizienter teilen lassen. Bit Torrent ist ein sogenanntes Peer-to-Peer-File-Sharing-Programm, was bedeutet, dass jeder Computer, der einen Teil einer Ressource herunterlädt, diesen Teil auch allen anderen zum Herunterladen anbietet, die auf diesen Teil zugreifen wollen. Dieses P2P-Modell bewirkt, dass ein Download umso schneller vonstattengeht, je beliebter eine Ressource ist. Eine Folge von *Game of Thrones* können Sie beispielsweise in wenigen Sekunden herunterladen, bei einer Kopie von *Liebe mit Risiko – Gigli* hingegen müssen Sie womöglich tagelang warten. Abbildung 21.46 zeigt eines der verbreiteteren Bit-Torrent-Programme namens *Deluge*. Für Bit Torrent gibt es auch viele legale Anwendungsmöglichkeiten, so ist es beispielsweise bei der Verteilung großer Dateien äußerst effizient und zur bevorzugten Methode für die Verteilung von Linux-Distributionen geworden. Es wird sogar zum Verteilen von Blizzard-Spielen (und den dazugehörigen Patches) verwendet, wie etwa *World of Warcraft* oder *Starcraft*! Die Bit-Torrent-Nutzer benötigen allerdings nach wie vor die Möglichkeit, Anbieter für die gesuchten Dateien zu finden, und Websites, die solche Listen anbieten, sind immer wieder Gegenstand von Gerichtsverfahren.

Nach all den rechtlichen Schritten hat sich das Geschäftsmodell der Inhaltanbieter in den letzten Jahren offenbar dahin gehend entwickelt, die Situation zu entschärfen, indem sie den Kunden bessere Zugriffsmöglichkeiten auf digitale Inhalte bieten. Früher waren die Möglichkeiten, online an digitale Inhalte zu gelangen, fast ausnahmslos illegal. In den letzten Jahren haben legale Streaming-Dienste wie Netflix, HBO oder Spotify (Abbildung 21.47) für die Kunden legale Möglichkeiten geschaffen, an

die gewünschten Inhalte zu gelangen, ohne dass sie physische Medien kaufen müssen (oder sogar das Risiko eingehen, statt der gewünschten Datei Schadsoftware herunterzuladen).

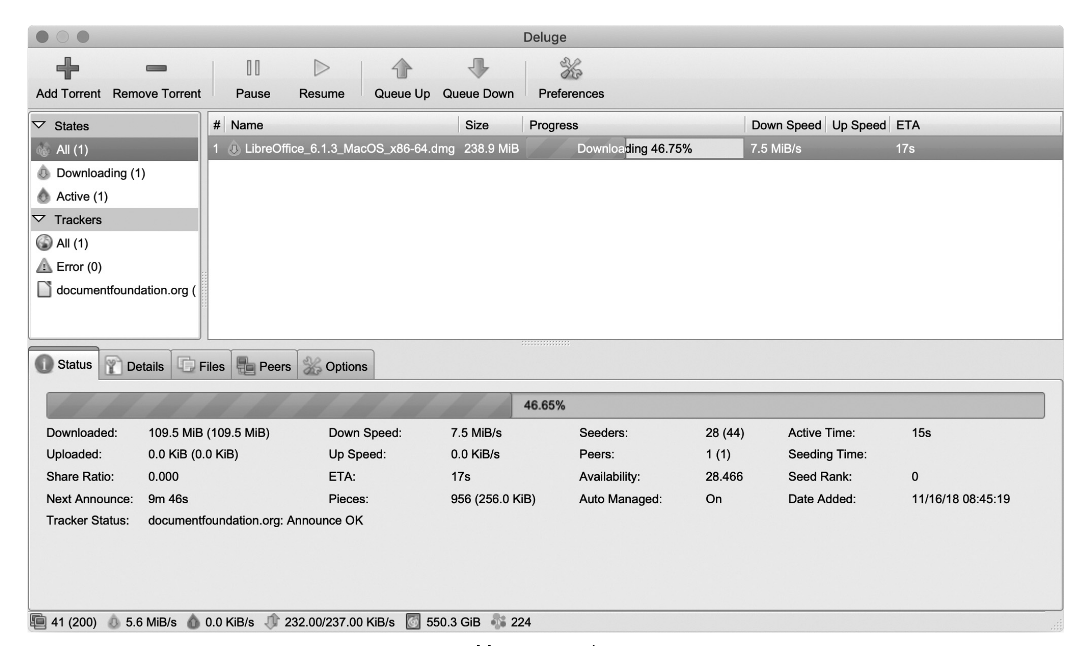


Abb. 21.46: Deluge

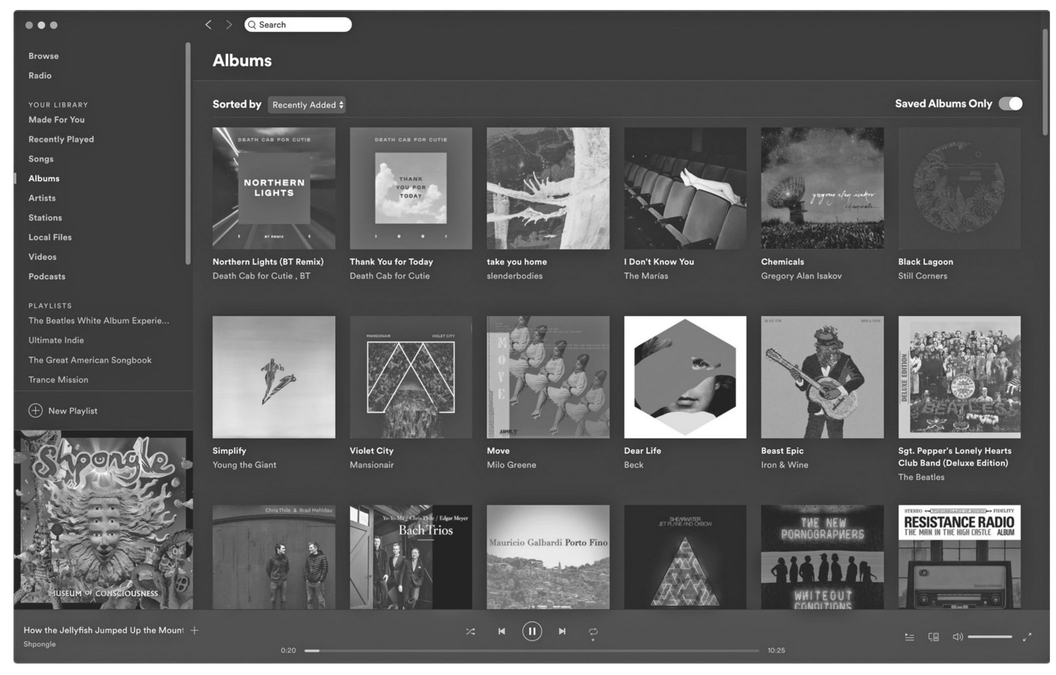


Abb. 21.47: Eine vielseitige Auswahl von Alben bei Spotify

Die genannten Beispiele kratzen nur an der Oberfläche der vielen Anwendungen, die das Internet nutzen. Einer der interessanten Aspekte von TCP/IP ist, dass das grundlegende Design rund 40 Jahre alt ist. Wir verwenden TCP/IP auf eine Art und Weise, die von den Entwicklern niemals vorgesehen war, dennoch zeigt es weiterhin seine Leistungsstärke und Flexibilität. Das ist schon erstaunlich!

21.3.10 Internet-Dienstprogramme

In den Lernzielen der CompTIA A+-Zertifizierungsprüfung 1002 werden fünf besondere Protokolle erwähnt. Bei zweien davon, nämlich LDAP und SNMP, bezweifle ich, dass Sie jemals näher damit in Berührung kommen werden. Das dritte, SMB, findet eher in LANs Einsatz, nicht im Internet. Das vierte Protokoll namens AFP betrifft nur macOS. Und das fünfte, SLP, ist vor allem bei netzwerkfähigen Druckern gebräuchlich. Dessen ungeachtet sollten Sie ein wenig über diese fünf Protokolle wissen.

LDAP

Mittels *LDAP* (*Lightweight Directory Access Protocol*) können Betriebssysteme und Anwendungen auf Verzeichnisdienste zugreifen. Wenn Sie beispielsweise einen Windows-Server mit Active Directory betreiben, verwendet Windows LDAP, um auf das Active Directory zuzugreifen. Wenn Sie dem Active Directory einen Computer hinzufügen, wird ebenfalls LDAP eingesetzt, um die Informationen zu aktualisieren. LDAP tritt nicht weiter in Erscheinung, leistet aber wichtige Dienste für das reibungslose Funktionieren des Verzeichnisdienstes.

SNMP

Mit *SNMP* (*Simple Network Management Protocol*) lassen sich alle möglichen Netzwerkgeräte überwachen und konfigurieren. Falls all Ihre Computer, Switches, Router usw. SNMP-fähig sind, können Sie spezielle Programme dazu verwenden, eine unglaubliche Menge an Informationen über das Netzwerk abzufragen. SNMP ist ein beliebtes Werkzeug, gehört jedoch zu den Dingen, die Sie vermutlich nicht verwenden müssen, wenn Sie kein Netzwerktechniker sind.

SMB

SMB (*Server Message Block*) ist das Protokoll zur Datei- und Druckerfreigabe in Windows. UNIX und Linux nutzen ein ähnliches Protokoll namens *NFS* (*Network File System*), das jedoch kaum noch in Gebrauch ist. Heutzutage verwenden alle bedeutenden Betriebssysteme SMB: Windows, macOS und Linux (in Form von SAMBA). Wenn es um Dateiserver im LAN geht, ist SMB das Protokoll der Wahl.

Wichtig

Im Laufe der Jahre hat Microsoft verschiedene SMB-Versionen vorgestellt (sogenannte *Dialekte*). Einer der verbreiteteren Dialekte trägt den Namen *CIFS* (*Common Internet File System*). CIFS gilt inzwischen zwar als veraltet, wird aber noch in hohem Maße unterstützt, daher sollten Sie es für die CompTIA A+-Prüfung kennen.

AFP

Microsoft hatte SMB und auch Apple entwickelte Ende der 1980er-Jahre ein Protokoll namens *AFP* (*Apple Filing Protocol*), um den Datenaustausch in den ersten lokalen Netzwerken zu ermöglichen. Ähnlich wie SMB hat auch AFP bis heute überlebt und dient dazu, Daten zwischen alten und neuen Macs auszutauschen. AFP ist außerdem das von Time Machine verwendete Protokoll zum Erstellen von Backups über das Netzwerk, da es die Besonderheiten des HFS+-Dateisystems unterstützt. Neben macOS unterstützt auch Linux AFP sehr gut. Windows hingegen unterstützt das Protokoll von Haus aus nicht.

1001

21.4 Das Internet der Dinge

Immer mehr Geräte sind mit dem Internet verbunden, um uns das Leben etwas einfacher zu machen und uns besser zu verbinden, und sind einfach nur cool. Dazu gehören alle möglichen Geräte: Kühlschränke, Thermostate, Lichtschalter, Überwachungskameras, Türschlösser und digitale Assistenten. Wir können auf diese Geräte über das Internet zugreifen, sie konfigurieren und Befehle erteilen. Zusammengenommen bilden sie das Internet der Dinge (*Internet of Things*, IoT). Die Konfigurationsmöglichkeiten dieser *smarten Geräte* sind je nach Hersteller oder Softwareentwickler völlig verschieden, deshalb ist es unmöglich, hier alle Geräte vorzustellen. Wir betrachten drei Beispiele, damit Sie einen Eindruck davon gewinnen, was man mit IoT-Geräten anstellen kann: Thermostate, Beleuchtung und digitale Assistenten. Dann werfen wir einen Blick auf die Protokolle, die bei der Hausautomation, also der Nutzung von IoT-Geräten, zum Einsatz kommen.

21.4.1 Hausautomation: Thermostate

Einen smarten Thermostaten können Sie von einem mit dem Internet verbundenen Gerät steuern, etwa mit dem Computer im Büro oder auf dem Heimweg von der Arbeit mit dem Smartphone. Abbildung 21.48 zeigt einen smarten Thermostaten.



Abb. 21.48: Smarter Thermostat von Honeywell

Zur Einrichtung solch eines Geräts sind einige einfache Schritte erforderlich. Sie müssen das Gerät mit einem WLAN verbinden. Das erfolgt am Gerät selbst, das nach Netzwerken sucht. Wählen Sie das richtige aus und geben Sie das Kennwort ein. Höchstwahrscheinlich benötigen Sie ein Benutzerkonto beim Hersteller. Der Hersteller Honeywell verwendet eine Software namens *Total Connect Comfort*.

Nachdem Sie ein Benutzerkonto eingerichtet haben, müssen Sie das Konto mit dem Gerät verknüpfen. Dazu sind ebenfalls einige Schritte erforderlich. Um den hier genannten Thermostaten einzurichten, musste ich beispielsweise die MAC-Adresse sowie einige weitere Informationen eingeben. Nachdem die Honeywell-Server auf das Gerät zugreifen konnten, musste ich eine von Honeywell vorgegebene bestimmte Temperatur einstellen, damit sie überprüfen konnten, dass ich physischen Zugang zu dem Thermostaten hatte. Damit war die Einrichtung erfolgreich abgeschlossen. Ich installierte die App TOTAL CONNECT COMFORT auf meinem iPad und meldete mich an (Abbildung 21.49). Jetzt kann ich meine Heizung und Klimaanlage von überall per Internet aus steuern.



Abb. 21.49: Fernsteuerung des Thermostaten

21.4.2 Hausautomation: Beleuchtung

Wer hätte gedacht, dass Beleuchtung so sexy sein kann? Viele Hersteller bieten smarte Beleuchtungssysteme zur Hausautomation an. Sie können von überall aus auf diese IoT-Geräte zugreifen und verschiedene Einstellungen vornehmen, etwa wann das Licht abends eingeschaltet oder tagsüber ausgeschaltet werden soll. Sie können auch automatisieren, dass die Beleuchtung im Laufe des Abends wärmeres Licht liefert. Beispielsweise kann am frühen Abend helles, bläuliches Licht erwünscht sein, das allmählicher immer dunkler und wärmer wird, damit man schläfrig wird. Abbildung 21.50 zeigt Apples HomeKit, das die Wohnzimmerbeleuchtung per Smartphone steuert. Ist das nicht klasse?



Abb. 21.50: Fernsteuerung der Beleuchtung per Internet

21.4.3 Digitale Assistenten

Ich: »Alexa! Spiel Songs von Jesse Cook.«

Alexa: »Ich wähle Songs von Jesse Cook bei Amazon Music aus.«

[Der Raum wird von großartigen Flamenco-Gitarrenklängen erfüllt.]

Die großen Vier (Amazon, Apple, Google und Microsoft) haben erstaunliche sprachgesteuerte digitale Assistenten entwickelt, um Ihr Zuhause auf vielfältige Weise mit dem Internet zu verbinden. Amazons Echo beispielsweise ermöglicht den Zugriff auf Ihr Amazon-Benutzerkonto, den Zugang zu gekaufter Musik, kann Informationen aus dem Internet abrufen und vieles mehr, und das alles, indem Sie »Alexa!« sagen und weitere Anweisungen geben (Abbildung 21.51).



Abb. 21.51: Echo Dot

Fragen Sie Apples Siri nach dem morgigen Wetter oder nach Wahlergebnissen in anderen Staaten. Sie wird klar und präzise antworten. Mit »Hey Google« gelangen Sie auf vergleichbare Weise an eine Antwort von Googles Smart-Home-Geräten. Microsoft hat eine Anlehnung in der Welt der Spiele gemacht und Cortana (aus dem bekannten Spiel *Halo*) als digitale Assistentin entwickelt. Bei Microsoft-Geräten beantwortet Cortana Fragen ebenso bereitwillig.

Die Einrichtung der digitalen Assistenten ist unkompliziert. Verbinden Sie Ihr Gerät mit dem lokalen WLAN und melden Sie sich mit einem Webbrowser am Gerät an, um eine Personalisierung vorzunehmen. Sobald Sie das Gerät mit dem Herstellerkonto verknüpft haben, ist es betriebsbereit und erleichtert Ihnen das Leben.

21.4.4 Protokolle: Z-Wave und Zigbee

Bei der Verwendung drahtloser Technologien zur Hausautomation gibt es eine Reihe von Herausforderungen. Zum einen ist da die große Anzahl von IoT-Geräten, die ein moderner Haushalt potenziell nutzen kann: Thermostate, Waschmaschinen, Steckdosen, Lampen und so weiter. Zum anderen gibt es in Privathaushalten im Gegensatz zu Firmengebäuden oft viele kleine Zimmer, enge Treppen und andere Hindernisse, die eine drahtlose Vernetzung erschweren. Die Nachfrage nach Hausautomation ist dennoch groß, und zwei konkurrierende Technologien, Z-Wave und Zigbee, liefern sich bei der drahtlosen Hausautomation ein Kopf-an-Kopf-Rennen. Z-Wave ist ein proprietärer Standard (mit einer öffentlichen API für Programmierer), Zigbee hingegen ist ein völlig offener Standard. Beide Standards verwenden eine Mesh-Netzwerktopologie, um die Kommunikation in Privathaushalten zu vereinfachen, und beide nutzen Hubs, die dazu dienen, das Netzwerk zu erweitern.

21.5 Fehlerbehebung bei Internetverbindungen

Es gibt niemanden, der mehr als ein paar Stunden im Internet verbracht hat und nicht auf irgendeine Form von Verbindungsproblem gestoßen ist. Wenn mich jemand anruft und sagt: »Das Internet funk-

tioniert nicht!«, mache ich mir immer einen Spaß daraus, zu antworten: »Nein, das Internet funktioniert bestens. Was nicht funktioniert, ist die Art und Weise, wie die Verbindung hergestellt wird.« Nun ja, vermutlich mache ich mir nicht gerade viele Freunde mit dieser Bemerkung, aber tatsächlich trifft sie, was die Ursachen für Verbindungsprobleme betrifft, den Nagel auf den Kopf. Lassen Sie uns nun die typischen Symptome untersuchen, die von der CompTIA in den Lernzielen aufgeführt werden, und betrachten, wie man diese nur allzu häufigen Probleme behebt.

Typischerweise besteht ein kleines Heimnetzwerk aus irgendeinem kleinen Kästchen (Kabelmodem, DSL-Modem usw.), das der ISP liefert und an das per Ethernet ein Router angeschlossen wird. Der Router ist meist WLAN-fähig und besitzt einige Ethernet-Anschlüsse, für gewöhnlich vier. Einige Computer sind per Kabel verbunden, andere via Drahtlosnetzwerk (Abbildung 21.52). Man kann wohl davon ausgehen, dass der CompTIA ein so aufgebautes Netzwerk vorschwebt, wenn es um die Fehlerbehebung bei Internetverbindungen geht, und wir wollen es ebenso halten.



Abb. 21.52: Ein typisches kleines Netzwerk

Eine letzte Bemerkung, bevor wir loslegen: Die meisten Internetverbindungsprobleme betreffen Schwierigkeiten bei der Verbindung von Netzwerken. Anders ausgedrückt: Alles in Kapitel 19 Erwähnte gilt auch hier, daher möchte ich die dort bereits erläuterten Probleme nicht nochmals aufbereiten. Die im Folgenden beschriebenen Aspekte beziehen sich nur auf Internetprobleme. Lassen Sie sich also nicht durch ein defektes Kabel täuschen und größere Probleme vermuten, als tatsächlich vorhanden sind.

21.5.1 Kein Zugang

Wie Sie aus Kapitel 19 wissen, kann »Kein Zugang« zweierlei Bedeutung besitzen: eine unverbundene Netzwerkkarte oder die Unmöglichkeit, auf eine Ressource zuzugreifen. Da in Kapitel 19 und 20 die kabelgebundenen bzw. drahtlosen Aspekte bereits beleuchtet wurden, will ich nun den fehlenden Zugang aus einer »Ich bin im Internet, aber kann eine Website nicht erreichen«-Perspektive betrachten:

1. Können Sie andere Websites erreichen? Falls nicht, überprüfen Sie erneut Ihre lokalen Verbindungen.
2. Können Sie die Site anpingen? Begeben Sie sich zur Kommandozeile und versuchen Sie, die URL wie folgt anzupingen:

```
C:\>ping www.cheetos1.com
Ping-Anforderung konnte Host "www.cheetos1.com" nicht finden. Überprüfen
Sie den Namen, und versuchen Sie es erneut.
C:\>
```

Das Anpingen hat zwar nicht funktioniert, aber wir lernen eine Menge daraus. Die Fehlermeldung beim Ping besagt, dass der Computer keine IP-Adresse für die Website finden kann. Das ist ein Hinweis auf einen DNS-Ausfall, ein häufiger Fehler. Versuchen Sie dann Folgendes:

- Geben Sie in Windows auf der Kommandozeile `ipconfig /flushdns` ein:

  ```
  C:\>ipconfig /flushdns
  Windows-IP-Konfiguration
  Der DNS-Auflösungscache wurde geleert.
  C:\>
  ```

- Öffnen Sie in Windows 10 die Einstellungen, wählen Sie NETZWERK UND INTERNET und klicken Sie auf ADAPTEREINSTELLUNGEN ÄNDERN. Klicken Sie nun mit der rechten Maustaste auf die Netzwerkverbindung und wählen Sie DIAGNOSE, um die Fehlerbehebung zu starten (Abbildung 21.53).
- Probieren Sie einen anderen DNS-Server aus. Es gibt viele öffentlich zugängliche DNS-Server, wie beispielsweise diejenigen von Google mit den IP-Adressen 8.8.8.8 und 8.8.4.4.

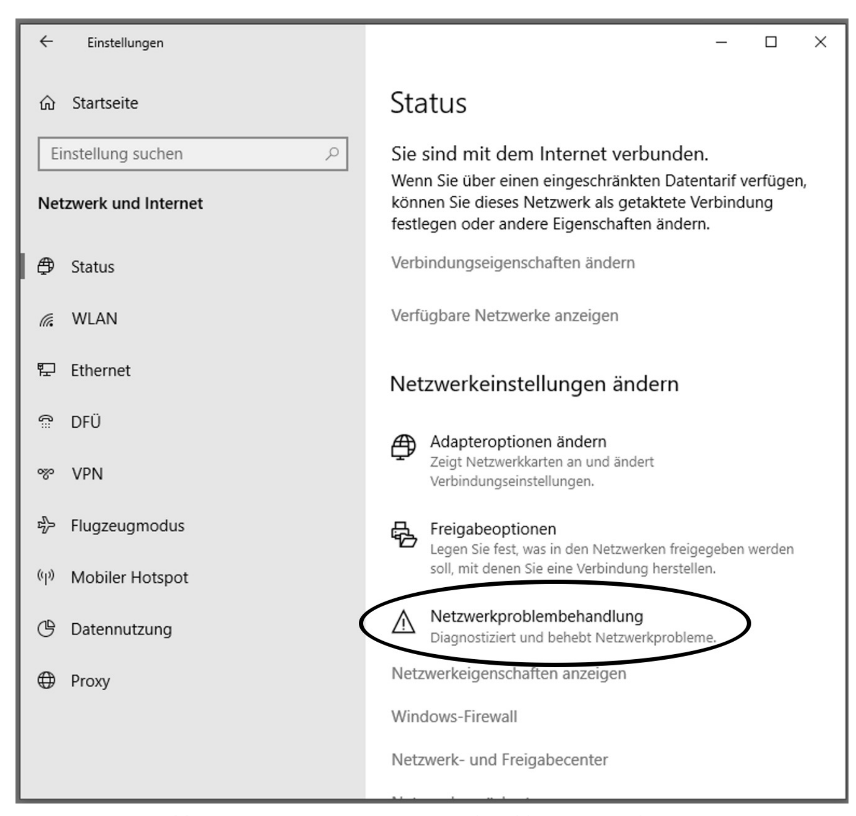


Abb. 21.53: Diagnose eines Netzwerkproblems in Windows 10

Hinweis

Die Befehle ähneln einander zwar, aber in macOS und Linux sind `ifconfig` und `iwconfig` nicht dazu geeignet, den DNS-Cache zu leeren.

Falls der DNS-Server ordnungsgemäß arbeitet, sollten Sie sicherstellen, dass die URL korrekt ist. Das gilt insbesondere bei der Eingabe von DNS-Namen in Anwendungen wie E-Mail-Programmen.

Wichtig

In der CompTIA A+-Prüfung 1001 können Fragen zu nicht verfügbaren Ressourcen vorkommen, wie etwa nicht funktionierender Internet- und E-Mail-Zugang. Berücksichtigen Sie bei Ihrer Antwort, dass die Verbindungen geprüft werden müssen oder dass es Konfigurationsprobleme geben könnte, wie hier beim DNS.

21.5.2 Beschränkter Zugang

Ein beschränkter Zugang deutet auf ein DHCP-Problem hin, sofern Sie Ihre IP-Adresse per DHCP beziehen. Führen Sie `ipconfig` aus, um zu überprüfen, ob Ihr Rechner eine APIPA-Adresse besitzt:

```
C:\>ipconfig
Windows-IP-Konfiguration
Ethernetadapter LAN-Verbindung
   Verbindungsspezifisches DNS-Suffix:
   IP-Adresse. . . . . . . . . . . . : 169.254.0.16
   Subnetzmaske. . . . . . . . . . . : 255.255.0.0
Standardgateway. . . . . . . . . . :
C:\>
```

Aha! Kein DHCP-Server! Falls Ihr Router gleichzeitig Ihr DHCP-Server ist, sollten Sie versuchen, das Gerät neu zu starten. Wenn Ihnen die Netzwerk-ID des Netzwerks und die IP-Adresse des Standardgateways bekannt sind (bei Ihrem eigenen Netzwerk sollten Sie das wirklich wissen), können Sie der Netzwerkkarte eine statische IP-Adresse zuweisen.

21.5.3 Nur lokaler Zugang

Nur lokaler Zugang bedeutet, dass Sie zwar auf Netzwerkressourcen zugreifen können, nicht aber aufs Internet. Hierbei handelt es sich um das klassische Symptom für einen ausgefallenen DHCP-Server, da alle lokalen Systeme APIPA- bzw. link-lokale Adressen erhalten. Möglicherweise liegt aber doch ein Problem beim Router vor. Pingen Sie das Standardgateway an. Funktioniert das, pingen Sie auch den WAN-Anschluss des Routers an. Dessen IP-Adresse müssen Sie über die Konfigurations-Webseiten herausfinden (Abbildung 21.54). An welchem Ort genau die Adresse steht, ist bei jedem Router anders – viel Glück bei der Suche!

Die WAN-IP-Adresse des Routers kann sehr aufschlussreich sein. Betrachten Sie Abbildung 21.55. Auf den ersten Blick sieht sie aus wie Abbildung 21.54, beachten Sie aber, dass es hier keine IP-Adresse gibt. Die meisten ISPs vergeben keine statischen IP-Adressen. Sie stellen Ihnen eine Verbindung zur Verfügung und der Netzwerkkarte Ihres Routers wird über DHCP eine IP-Adresse zugewiesen, ebenso wie in den meisten internen Netzwerken. Wenn Sie Glück haben, können Sie die DHCP-Adresse mittels einer Schaltfläche auf den Konfigurationsseiten des Routers erneuern. Steht diese Funktion nicht zur Verfügung, sollten Sie das Kabel- oder DSL-Modem zurücksetzen. Hilft auch das nicht, ist es an der Zeit, Ihren ISP anzurufen.

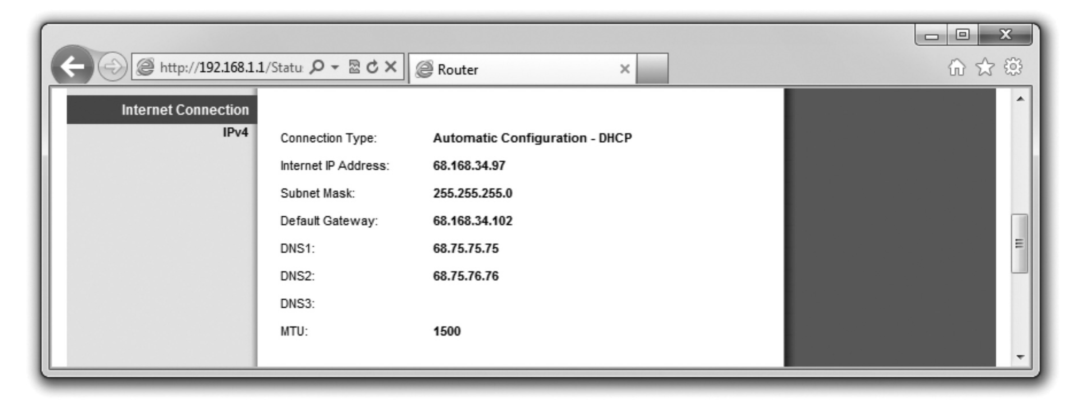


Abb. 21.54: Die WAN-IP-Adresse eines Routers

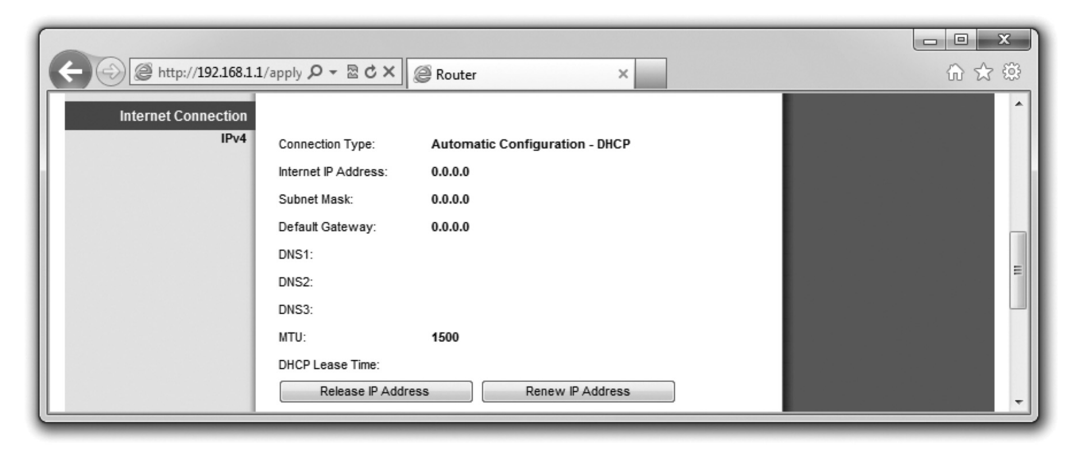


Abb. 21.55: Keine WAN-Verbindung

21.5.4 Geringe Datenübertragungsrate

Es spielt keine Rolle, wie schnell die Internetverbindung ist, sie kann gar nicht schnell genug sein. Die Leute sind es gewohnt, dass der Start umfangreicher Programme oder das Laden eines hochauflösenden Videos eine gewisse Zeit in Anspruch nimmt, aber es kommt vor, dass die Geschwindigkeit der Internetverbindung tatsächlich unzumutbar langsam wird.

Nun besitzt Ihre Internetverbindung ja eine maximale Geschwindigkeit, mit der Daten übertragen werden können. Wenn die Verbindung von mehreren Programmen gleichzeitig verwendet wird, steht jedem einzelnen Programm nur noch eine geringe Bandbreite zur Verfügung. Geben Sie auf der Kommandozeile das Kommando `netstat` ein, um anzuzeigen, was gerade im Netzwerk vor sich geht. Es werden sämtliche Netzwerkverbindungen zwischen Ihrem Computer und anderen Geräten aufgelistet. Hier eine etwas vereinfachte Ausgabe des Kommandos:

```
C:\>netstat
Aktive Verbindungen
Proto Lokale Adresse      Remoteadresse         Status
TCP   10.12.14.47:57788   totalfs3:microsoft-ds HERGESTELLT
TCP   192.168.15.102:139  Sabertooth:20508      HERGESTELLT
```

```
TCP   192.168.15.102:50283 Theater:netbios-ssn   HERGESTELLT
TCP   192.168.15.102:60222 dts1.google.com:https HERGESTELLT
TCP   192.168.15.102:60456 www.serv2.le.com:http HERGESTELLT
TCP   192.168.15.102:60482 64.145.92.65:http     HERGESTELLT
TCP   192.168.15.102:60483 12.162.15.1:57080     WARTEND
C:\>
```

Wenn Sie sich die Spalte `Remoteadresse` genauer ansehen, stellen Sie fest, dass es sich bei den meisten Verbindungen um Webseiten (`HTTP` und `HTTPS`) oder Ordnerfreigaben (`microsoft-ds`, `netbios-ssn`) handelt. Aber was ist `12.162.15.1:57080`? Da ich auch nicht sämtliche Verbindungstypen auswendig kenne, habe ich danach gegoogelt und herausgefunden, dass auf meinem Rechner im Hintergrund ein Torrent-Client lief. Ich habe das Programm gefunden und beendet.

Wenn alle Benutzer im Netzwerk über geringe Verbindungsgeschwindigkeiten klagen, sollten Sie sich den Router ansehen. Höchstwahrscheinlich brauchen einfach zu viele Benutzer zu viel Bandbreite – Sie brauchen eine schnellere Internetverbindung!

Wenn der Zukauf von Bandbreite nicht infrage kommt, müssen Sie aus der vorhandenen Bandbreite das Beste machen. Mittels *QoS* (*Quality of Service*) können Sie steuern, was durch Ihren Router hindurchgeleitet wird. Mit dieser Funktion lässt sich die Bandbreite für bestimmte Arten von Daten anhand des Anwendungsprotokolls, der IP-Adresse und vieler weiterer Kriterien beschränken. Abbildung 21.56 zeigt eine typische QoS-Konfigurationsseite eines Routers

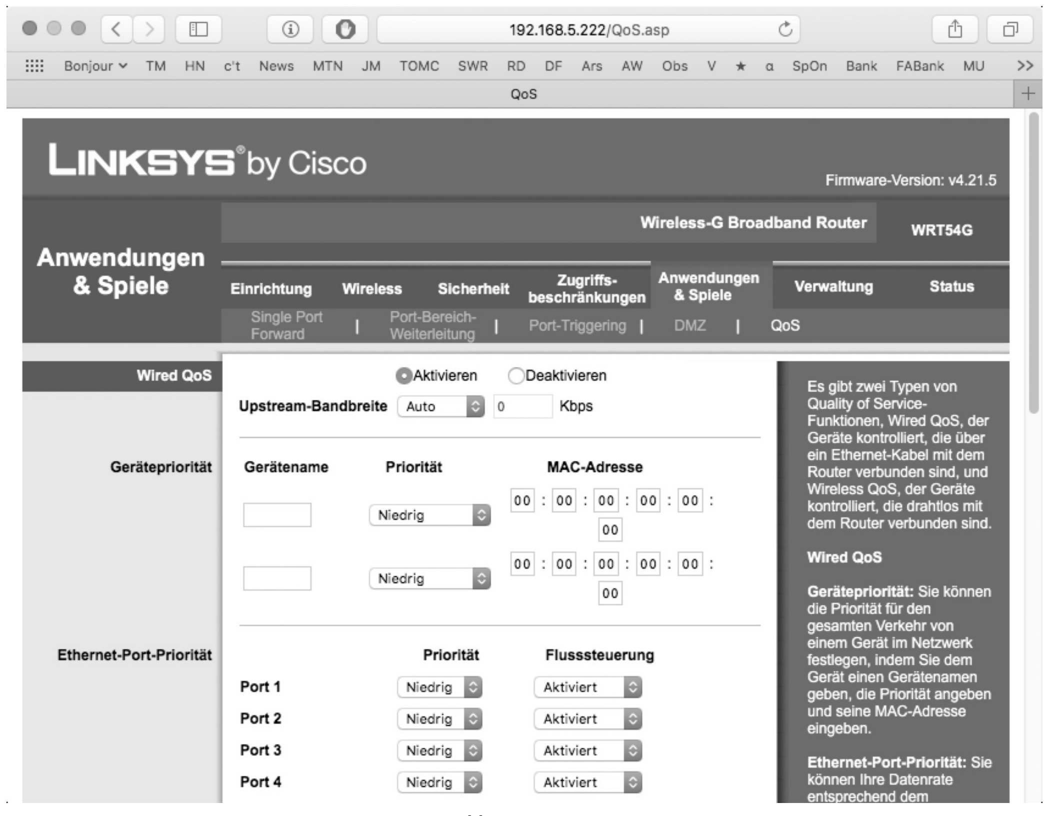


Abb. 21.56: QoS

Jenseits von A+

Die von den CompTIA A+-Zertifizierungsprüfungen abgedeckten Bereiche beschäftigen sich mit den allgemeinen Aspekten des Internets. Es gibt jedoch ein Thema, das zwar über die CompTIA A+-Prüfungen hinausgeht, aber derart verbreitet und wichtig ist, dass es Ihnen vertraut sein sollte: Online-Spiele.

21.5.5 Online-Spiele

Online-Spiele gehören zu den aufregenderen Aspekten des Internets – und sie machen natürlich auch Spaß! Online gegen eine reale Person zu spielen, macht einfach Freude. Klassiker wie Hearts und Backgammon sind eine interessante Herausforderung. Ein weiteres beliebtes Genre der Online-Spiele sind die immer wieder kontrovers diskutierten sogenannten *Ego-Shooter*. Bei diesen Spielen bewegen sie sich innerhalb einer kleinen Welt mit bis zu 64 anderen Spielern. Ein gutes Beispiel dafür ist *Counter-Strike: Global Offensive* von *Valve Software* (Abbildung 21.57).



Abb. 21.57: Counter-Strike: GO

Die Diskussion der Online-Spiele wäre nicht vollständig, würde man nicht auf den erstaunlichsten Spieletyp überhaupt hinweisen, die *MMORPGs* (*Massively Multiplayer Online Role-Playing Game*). Stellen Sie sich vor, Sie sind ein Blutelf, der begleitet von einer ganzen Horde Freunde auf Abenteuer in Welten geht, die so groß sind, dass Sie einen ganzen Tag bräuchten, um durch sie zu reisen. In derselben Welt sind 2.000 oder 3.000 andere Spieler und Tausende von dem Spiel gesteuerte Charaktere anwesend! Es gibt viele MMORPGs, aber das wohl beliebteste ist heute *World of Warcraft* (Abbildung 21.58). Beachten Sie, dass diese Spiele TCP/IP nutzen, um Daten über spezielle Ports zu übertragen, die für das Spiel reserviert werden.



Abb. 21.58: World of Warcraft

21.6 Wiederholung

21.6.1 Fragen

1. Welche der vier nachfolgend angegebenen Internetverbindungen ist normalerweise am langsamsten?
   A. Kabel
   B. Wählverbindung
   C. DSL
   D. Satellit
2. Welchen Port verwendet POP3?
   A. 22
   B. 110
   C. 42
   D. 256
3. Welchen Vorteil haben Wählverbindungen gegenüber DSL?
   A. Wählverbindungen sind schneller als DSL.
   B. Man darf weiter als 5,5 Kilometer von der nächsten Hauptvermittlungsstelle entfernt sein.
   C. Sie können eine zweite Telefonleitung nur für Wählverbindungen einrichten.
   D. Es gibt keinen. Wählverbindungen haben keine Vorteile gegenüber DSL.

4. Welches Protokoll können Sie zum Versenden von E-Mail verwenden?
   A. IMAP4
   B. POP3
   C. PPP
   D. SMTP
5. Welche Protokolle können Sie zum Empfangen von E-Mail verwenden? (Wählen Sie zwei Antworten aus.)
   A. IMAP4
   B. POP3
   C. PPP
   D. SMTP
6. Welchen Vorteil haben Satelliten gegenüber Kabel bei Internetverbindungen?
   A. Satelliten sind schneller als Kabel.
   B. Kabel ist bei schlechtem Wetter unzuverlässig, Satelliten nicht.
   C. Bei Satellitenverbindungen müssen Sie sich im Umkreis von 5,5 Kilometern der zentralen Hauptvermittlungsstelle befinden.
   D. Kabel ist auf Gebiete beschränkt, in denen auch Kabel installiert sind, Satelliten aber nicht.
7. Welche der Zuordnungen von Portnummer(n) und Protokoll sind **nicht** richtig? (Wählen Sie zwei Antworten aus.)
   A. 137, 138, 139, 445 = SMB
   B. 3398 = RDP
   C. 80 = HTTPS
   D. 22 = SSH
8. Welcher Befehl ermöglicht Ihnen häufig die Diagnose von TCP/IP-Fehlern, wie beispielsweise Verbindungsprobleme?
   A. FTP
   B. `ping`
   C. QoS
   D. APIPA
9. Welche der folgenden Mobilfunktechnologien wird für gewöhnlich als 4G angesehen?
   A. EDGE
   B. UMTS
   C. LTE
   D. CDMA
10. Welche der folgenden Programme ermöglichen es Ihnen, von Ihrem lokalen Computer aus auf einen entfernten Computer zuzugreifen und mit ihm zu arbeiten? (Wählen Sie zwei Antworten aus.)
   A. FTP
   B. DNAT
   C. Remotedesktopverbindung
   D. Telnet

21.6.2 Antworten

1. **B.** Wählverbindungen sind robust und allgemein verfügbar, aber viel langsamer als die neueren Verbindungstypen.
2. **B.** POP3 verwendet Port 110.
3. **B.** DSL ist auf die relativ kurze Entfernung von 5,5 km zu einem Haupt-Switch beschränkt, weshalb es in ländlichen Gebieten häufig nicht (oder nur mit Einschränkungen) genutzt werden kann. Für Wählverbindungen (DFÜ-Verbindungen) brauchen Sie nur eine Telefonleitung.
4. **D.** Sie können SMTP zum Versenden von E-Mail-Nachrichten verwenden.
5. **A, B.** Sie können entweder IMAP oder POP3 zum Empfang von E-Mail-Nachrichten verwenden.
6. **D.** Wenn Sie eine Satellitenverbindung benutzen, werden Sie natürlich unabhängig vom Kabel der Kabelbetreiber!
7. **B, C.** RDP (Remote Desktop Protocol) verwendet Port 3389. HTTPS (Hypertext Transfer Protocol Secure) verwendet Port 443, nicht Port 80, der von HTTP genutzt wird.
8. **B.** Häufig können Sie den Befehl `ping` zur Diagnose von TCP/IP-Problemen verwenden.
9. **C.** LTE (Long Term Evolution) wird im Allgemeinen als 4G-Mobilfunktechnologie betrachtet.
10. **C, D.** Mit Telnet und Remotedesktopverbindung können Sie auf einem an einem anderen Ort stehenden Rechner arbeiten. Die letztere Option ist allerdings komfortabler und sicherer!

Virtualisierung 22

Themen in diesem Kapitel:

- Warum man sich die Virtualisierung so gerne zu eigen macht
- Erstellen und Verwenden einer virtuellen Maschine
- Dienstebenen und Architekturen in der Cloud

Das Thema dieses Kapitels, die Virtualisierung, kann die Gehirnwindungen in Mitleidenschaft ziehen, wenn man es unvorbereitet angeht. Betrachten wir also ein Fallbeispiel. Mario hat gerade sein eigenes Unternehmen gegründet, das Websites hostet, und sein erster Kunde ist die Bayland Widgets Corporation. Was braucht Mario, um eine Website bereitzustellen? Dazu sind auf jeden Fall vier Dinge erforderlich:

- Ein Computer
- Ein Betriebssystem
- Webserver-Software
- Eine Internetverbindung

Mr. Schwarz, der IT-Leiter von Bayland Widgets, hat für die Software und Hardware zur Optimierung der Website seines Unternehmens ganz bestimmte Vorlieben und Abneigungen. Er möchte Rechner von Dell und ein Serverbetriebssystem von Microsoft einsetzen. Als Webserver soll Microsoft Internet Information Services (ISS) zum Einsatz kommen. Das wäre schon einmal der erste Rechner.

Ein zweiter Kunde erscheint, der IT-Leiter von Highland Gadgets Corporation, einer der Konkurrenten von Bayland Gadgets. Highland stellt jedoch andere Anforderungen an die Software. Mr. Barber, der IT-Leiter, bevorzugt zwar ebenfalls Computer von Dell, möchte aber als Betriebssystem Linux und als Webserver Apache verwenden.

Mario hat jetzt also zwei Computer, auf denen verschiedene Betriebssysteme und Webserver laufen, die zwei Netzwerkverbindungen benötigen und Strom verbrauchen. Das ist nicht besonders wirtschaftlich!

Zu allem Überfluss sind die beiden Dell-Maschinen auch bei Weitem nicht ausgelastet und haben noch jede Menge Rechenleistung übrig, weil die Websites noch nicht sehr viel Datenverkehr verursachen. Was für eine Verschwendung!

In der modernen IT wird dieses Dilemma mithilfe der *Virtualisierung* in Angriff genommen. Auf einem einzigen Rechner, dem Wirt,, läuft eine spezielle Software, die Umgebungen bereitstellt (die in getrennten Dateien gespeichert werden), die andere Rechner simulieren. Diese Betriebssystemumgebung wird als *virtuelle Maschine* (VM) oder als *Gast* bezeichnet.

Um die Probleme Unwirtschaftlichkeit und Verschwendung zu lösen, kann Mario auf einem der Computer mit Windows Server Virtualisierungssoftware installieren und dann eigenständige Windows- und Linux-Systeme betreiben, auf denen IIS bzw. Apache laufen. Die beiden Webserver werden sich nicht in die Quere kommen, weil sie in unterschiedlichen Dateien enthalten sind. Das ist das Prinzip der Virtualisierung.

Dieses Kapitel beschreibt die Virtualisierung ausführlich. Zunächst geht es darum, dass die Virtualisierung heutzutage von großer Bedeutung ist. Im nachfolgenden Abschnitt betrachten wir Implementierung der Virtualisierung in der Praxis. Das Kapitel endet mit Erläuterungen zum Cloud-Computing, den Anwendungen der Virtualisierung, die das Internet nutzen.

1001

22.1 Vorteile der Virtualisierung

Die Virtualisierung bietet Unternehmen enorme Vorteile. Hier sind die vier wichtigsten:

- Geringerer Energieverbrauch
- Konsolidierung der Hardware
- Systemverwaltung und Sicherheit
- Testsysteme

22.1.1 Geringerer Energieverbrauch

Bevor es die Virtualisierung gab, war für jedes installierte Betriebssystem ein eigener, physischer Rechner erforderlich. Mittels Virtualisierung können hingegen mehrere Betriebssysteme auf einem einzigen physischen System betrieben werden, wodurch die Energiekosten spürbar sinken. Statt auf einem Gerät einen Windows-Dateiserver, auf einem weiteren einen DNS-Server laufen zu lassen und auf einem dritten Rechner einen DHCP-Server unter Linux zu betreiben, reicht ein Computer aus, auf dem die drei Betriebssysteme gleichzeitig arbeiten (Abbildung 22.1).



Abb. 22.1: Virtualisierung ist energiesparend.

22.1.2 Konsolidierung der Hardware

Wie beim Energiesparen durch das Zusammenlegen mehrerer Server auf einen leistungsstarken Rechner kann man auch den Kauf teurer Hardware vermeiden, die während ihrer Lebensdauer kaum einmal ausgelastet ist. Komplexe Desktop-PCs können durch einfache, aber langlebige *Thin-Clients* ersetzt werden, die oft weder Festplatte noch Lüfter oder optische Laufwerke benötigen, weil sie nur leistungsfähig genug sein müssen, um auf einen entfernten Server zugreifen zu können. Hier stellt sich die Frage, warum man einen teuren Rechner mit mehreren Prozessoren, RAID-Verbund, redundanter Stromversorgung usw. ausstatten sollte, wenn letzten Endes nur ein einziger Server darauf läuft, der nur einen Bruchteil der Ressourcen nutzt. Dank Virtualisierung können Sie gleich eine ganze Reihe von Servern auf einem einzigen Computer betreiben.

22.1.3 Systemverwaltung und Sicherheit

Die vermutlich beliebtesten Gründe für eine Virtualisierung dürften die Vorteile sein, die man aus der vereinfachten Verwaltung des Systems zieht, denn VMs sind einfach nur Dateien und können wie alle

anderen Dateien auch kopiert werden. Neuen Mitarbeitern kann in Windeseile eine an die jeweilige Abteilung angepasste virtuelle Maschine bereitgestellt werden, auf der sämtliche benötigte Software bereits installiert ist.

Die Verwaltungsmöglichkeiten bieten zudem einen Vorteil hinsichtlich der Sicherheit. Angenommen, Sie haben für einen neuen Mitarbeiter ein herkömmliches System eingerichtet. Falls dieses System nicht mehr läuft, sei es durch Hacker, Malware oder wodurch auch immer, müssen Sie es mithilfe eines Backups wiederherstellen, das unter Umständen gar nicht so schnell zur Verfügung steht, oder eine Neuinstallation vornehmen. Bei der Virtualisierung werden der Wirtrechner, der Hypervisor und andere VMs *im Allgemeinen* nicht in Mitleidenschaft gezogen. Eine virtuelle Maschine können Sie einfach stoppen und sofort durch eine (nicht infizierte) Sicherungskopie ersetzen. Und da VMs einfache Dateien sind, kann man sie problemlos verwahren.

Wichtig

Ich schreibe hier *im Allgemeinen*, weil mit einem Netzwerk verbundene VMs den gleichen Risiken ausgesetzt sind (und ebenso eine Bedrohung darstellen können) wie alle anderen vernetzten Computer. Für vernetzte VMs gelten ähnliche Sicherheitsanforderungen wie für physische Systeme, und Sie sollten sie auch den gleichen Sicherheitsmaßnahmen unterziehen. Auch die Betriebssysteme und Anwendungen von VMs müssen regelmäßig aktualisiert werden und benötigen eine Firewall, sichere Kennwörter und dergleichen.

Die meisten virtuellen Maschinen bieten die Möglichkeit, sogenannte *Snapshots* oder *Sicherungspunkte* anzulegen, die eine exakte Kopie der virtuellen Maschine zum Zeitpunkt des Snapshots darstellen. Sie ermöglichen es, diesen Zustand schnell und einfach wiederherzustellen. Snapshots sind bestens als Absicherung geeignet, wenn möglicherweise riskante (oder auch weniger gefährliche) Wartungsarbeiten vorgenommen werden müssen. Sie sollten allerdings nicht als langfristige Backupstrategie eingesetzt werden, da sie die Performance beeinträchtigen können. Entfernen Sie den Snapshot, sobald die gefährliche Situation überstanden ist. Abbildung 22.2 zeigt VMware vSphere beim Erstellen eines Snapshots.

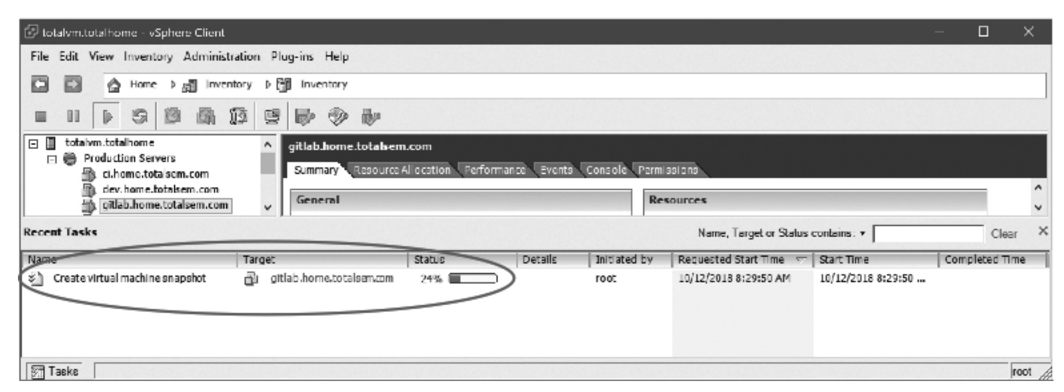


Abb. 22.2: Speichern eines Sicherungspunkts

Wichtig

Virtualisierte Betriebssysteme setzen die gleichen Schutzmaßnahmen wie echte Betriebssysteme ein. Die Namen, Kennwörter und Berechtigungen von Benutzerkonten auf virtuellen Maschinen müssen Sie wie bei normalen PCs im Auge behalten.

22.1.4 Testsysteme

Ein großartiges Beispiel für den Einsatz von Testsystemen entstammt meinem eigenen Unternehmen. Ich vertreibe ja Lehr- und Schulungssoftware mit Fragen aus der Praxis, um die eigenen Fähigkeiten zu testen und zur Prüfungsvorbereitung. Jedenfalls erhalte ich häufiger Supportanfragen und viele der geschilderten Probleme lassen sich oft nur mit der identischen Betriebssystemversion nachvollziehen. Bevor es die Virtualisierung gab, standen hier sieben bis zehn Rechner (Multiboot-Systeme) mit allen möglichen Windows-Versionen herum. Heute erlaubt mir ein einziger Hypervisor auf einem einzigen Rechner das Ausführen einer großen Anzahl verschiedener Betriebssystem-Versionen.

22.2 Implementierung der Virtualisierung

Wir sehen uns nun die heute gebräuchliche Implementierung der Virtualisierung an. Wir werden insbesondere verschiedene Betriebssysteme betrachten. Abbildung 22.3 zeigt ein Beispiel, nämlich ein Windows-System, auf dem ein Programm namens Hyper-V läuft, das zwei VMs ausführt: Auf einer läuft Ubuntu Linux, auf der anderen läuft Windows 10.

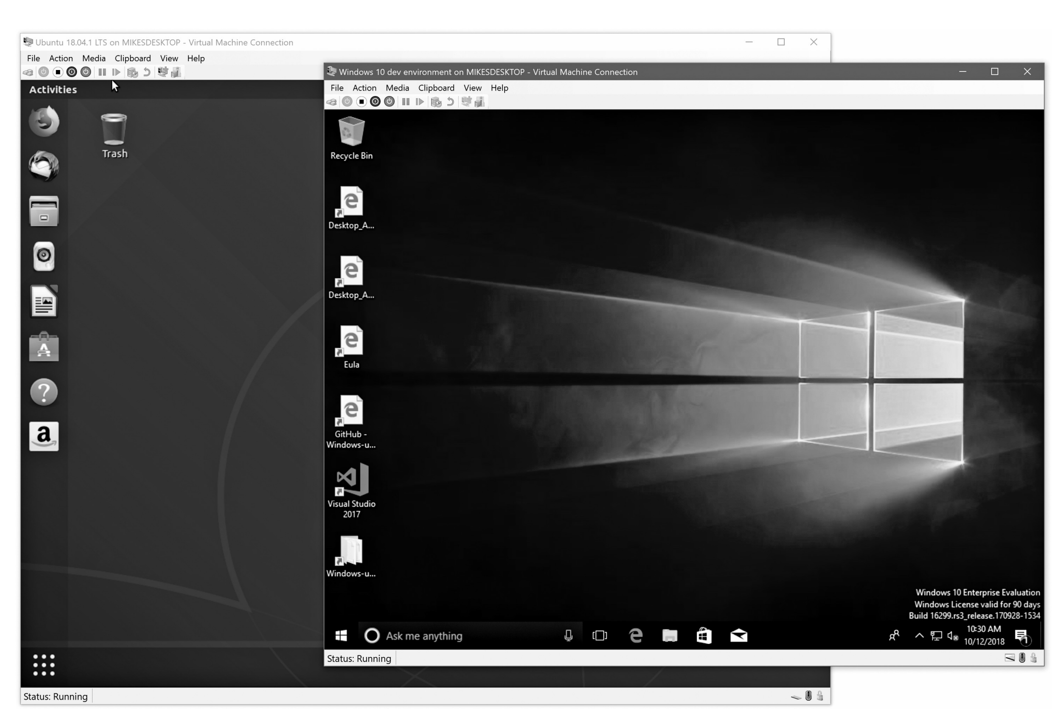


Abb. 22.3: Hyper-V führt Linux und Windows 10 aus.

22.2.1 Der Hypervisor

Ein normales Betriebssystem verwendet einen sogenannten *Supervisor*, um Funktionen und Prozesse auszuführen, mit denen so grundlegende Aufgaben wie die Zusammenarbeit zwischen Hardware und Software, Zuteilung der Rechenzeit und Speicherverwaltung erledigt werden. Abbildung 22.4 zeigt, wie der Supervisor zwischen Betriebssystem und der Hardware vermittelt.

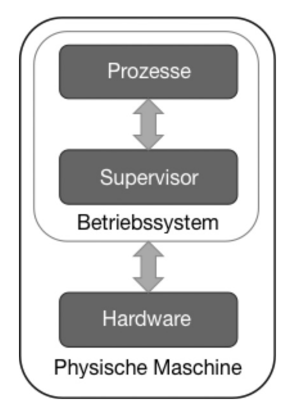


Abb. 22.4: Supervisor eines einzelnen Systems

Dank der Virtualisierung kann man auf einem einzelnen System, dem sogenannten *Wirt*, mehrere Gastbetriebssysteme gleichzeitig betreiben. Um das zu ermöglichen, ist eine weitere Softwareebene erforderlich, mit der die erheblich komplexeren Interaktionen gesteuert und verwaltet werden. Für diese Aufgaben ist der sogenannte *Hypervisor* zuständig. Abbildung 22.5 zeigt den Hypervisor eines einzelnen Systems, das drei verschiedene Gastbetriebssysteme beherbergt.

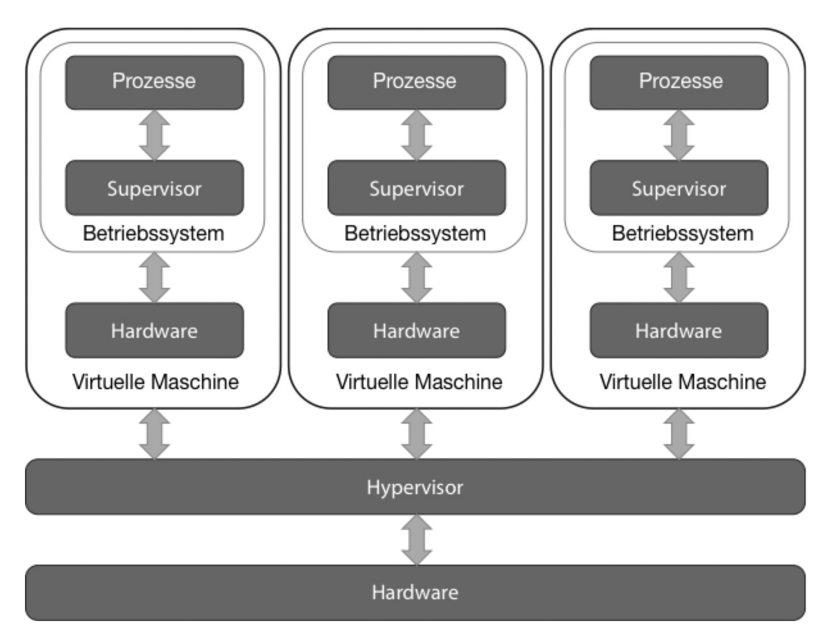


Abb. 22.5: Hypervisor eines einzelnen Wirtssystems mit drei virtuellen Maschinen

Es gibt verschiedene Hypervisor-Hersteller. Einer der ältesten und wohl derjenige, der letzten Endes der Virtualisierung zum Durchbruch verholfen hat, ist VMware (`http://www.vmware.com`). VMware hat schon 1999 die Software VMware Workstation für Windows und Linux veröffentlicht. Seitdem ist VMware rasant gewachsen und bietet heute eine umfangreiche Palette von Virtualisierungsprodukten an (Abbildung 22.6).

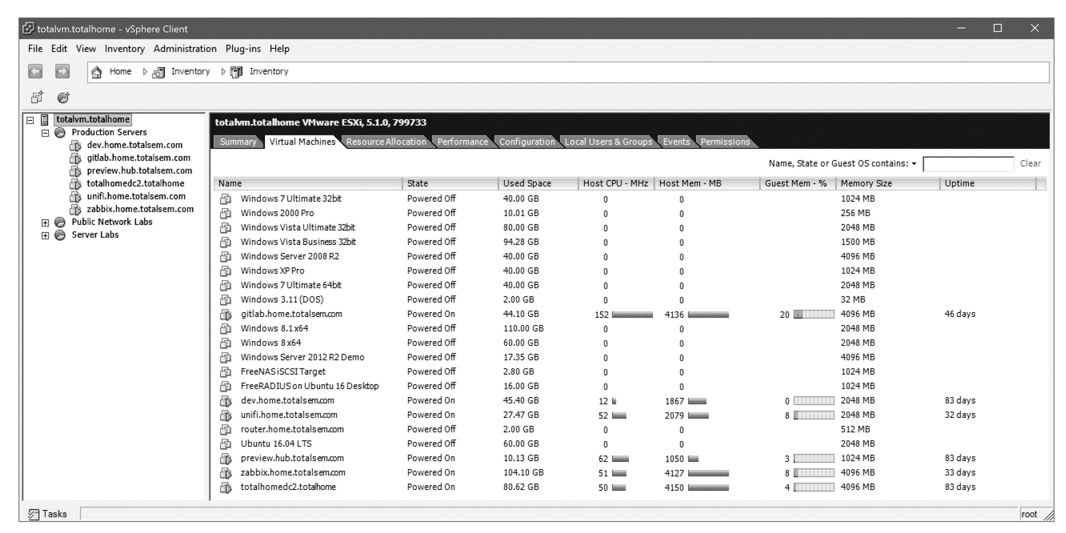


Abb. 22.6: Der gut ausgelastete VMware-Server des Autors

Microsofts Hyper-V wird mit den Serverversionen von Windows und seit Windows 8 Professional auch mit den Desktop-Versionen ausgeliefert. Hyper-V ist zwar nicht so verbreitet wie die Produkte von VMware, besitzt aber eine breite Anwenderbasis, die kontinuierlich wächst (Abbildung 22.7).

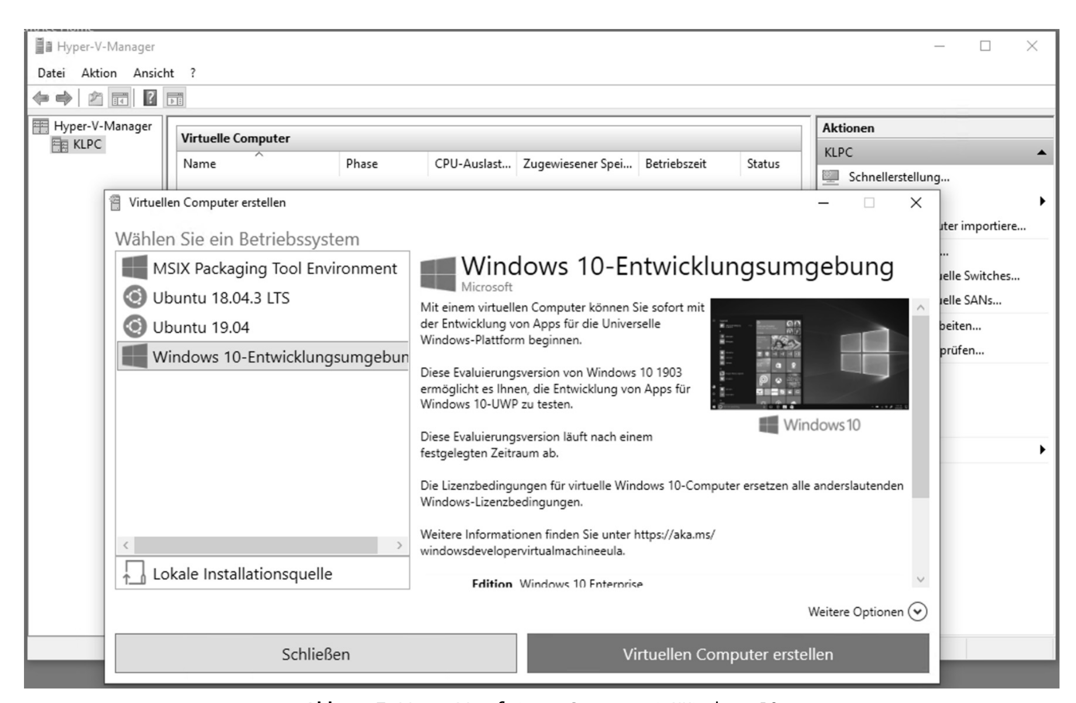


Abb. 22.7: Hyper-V auf einem System mit Windows 10

Ein weiterer sehr beliebter Hypervisor ist Oracles *VirtualBox* (Abbildung 22.8). Das leistungsfähige Programm ist für Windows, macOS und Linux zu haben.

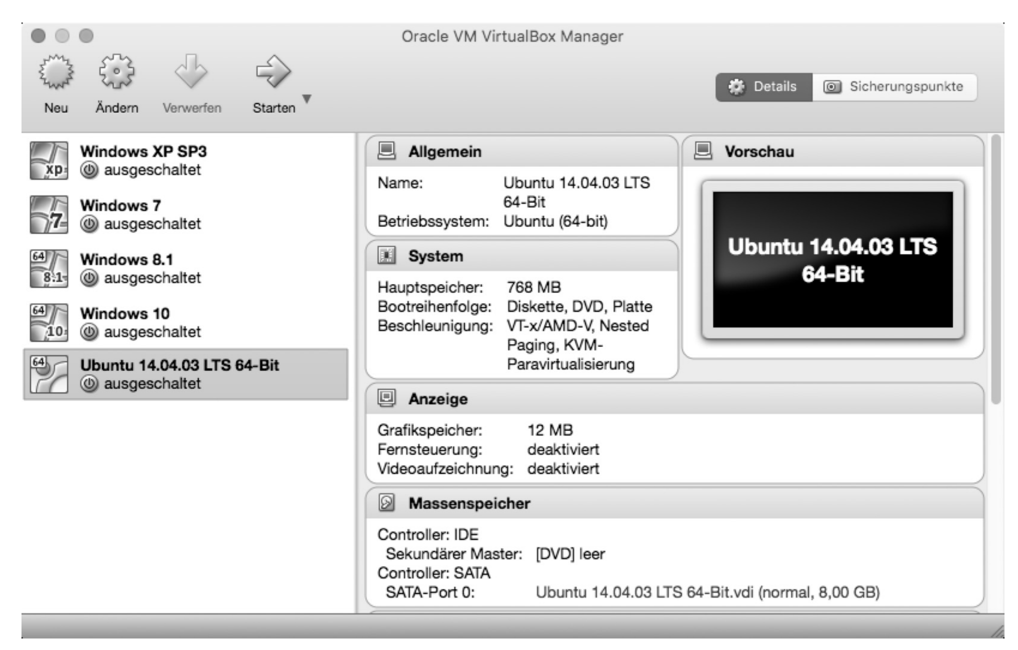


Abb. 22.8: Oracle VirtualBox

Bei den Anwendern von macOS sind die Hypervisoren VMware Fusion und Parallels Desktop (Abbildung 22.9) am beliebtesten. Beide Lösungen sind ebenfalls leistungsstark, aber im Gegensatz zu Hyper-V und VirtualBox nicht kostenlos.

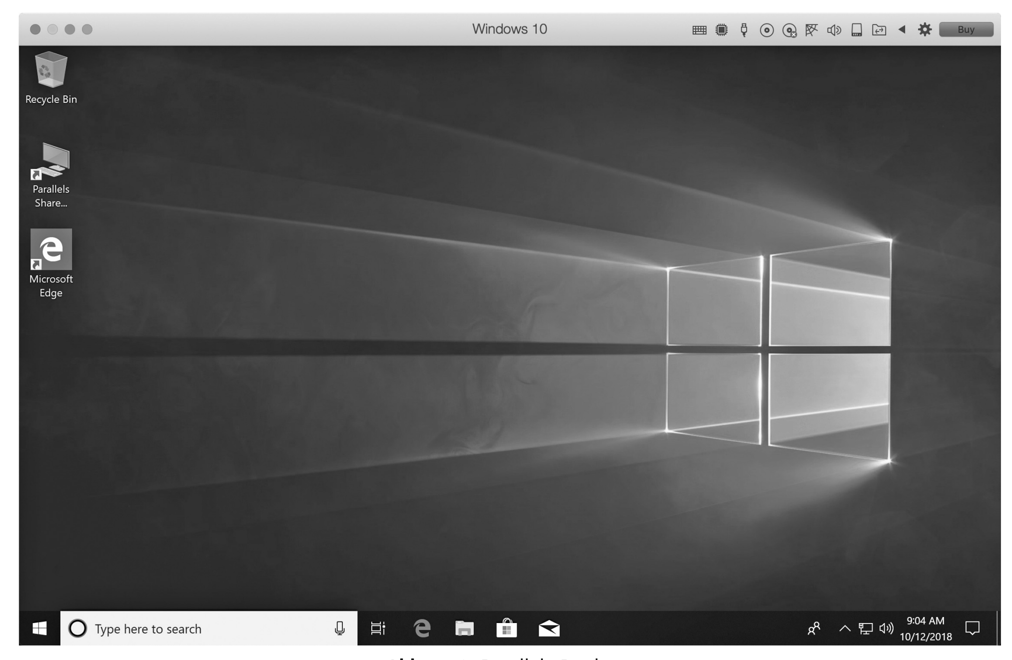


Abb. 22.9: Parallels Desktop

Damit ist die Liste verfügbarer Hypervisoren keineswegs vollständig. Beispielsweise schwören viele Linux-Anwender auf KVM, aber die hier vorgestellten Hypervisoren sind diejenigen, denen Sie in der Praxis am ehesten begegnen werden. Für die CompTIA A+-Zertifizierungsprüfung sollten Sie zumindest Microsofts Hyper-V kennen!

Hinweis

VMware stellte eine Reihe wirklich bemerkenswerter Virtualisierungsprodukte her, die allerdings ziemlich kostspielig sein können. Microsofts Hyper-V, KVM für Linux und Oracles VirtualBox sind hingegen kostenlos.

22.2.2 Emulation vs. Virtualisierung

Bei der Virtualisierung wird die Hardware des Wirtssystems gewissermaßen auf die verschiedenen virtuellen Maschinen aufgeteilt. Im Fall eines Intel-Systems erstellt der Hypervisor eine VM, die sich exakt wie das Intel-Wirtssystem verhält. Es ist nicht möglich, dass sich das Wirtssystem plötzlich wie eine andere Art von Computer mit anderem Prozessor verhält. Beispielsweise können Sie auf einem Intel-System keine virtuelle Maschine einer Nintendo 3DS erstellen. Der Hypervisor reicht nur den Code, der auf der VM laufen soll, an den echten Prozessor weiter.



Abb. 22.10: Ein Super-Nintendo-Emulator unter Windows

Die *Emulation* unterscheidet sich hier sehr von der Virtualisierung. Bei einem Emulator handelt es sich um Software oder Hardware, die Befehle und Kommandos einer völlig anderen Plattform mit anderem Prozessor so übersetzt, dass sie auf dem Wirtssystem ausgeführt werden können. Abbildung 22.10 zeigt ein Windows-System mit einem Emulator des Super Nintendo Entertainment Systems namens *Snes9X*, auf dem das Spiel *Donkey Kong Country* läuft.

Wichtig

Die CompTIA führt in den Lernzielen Emulation als Teil der Virtualisierung auf, obwohl sich die beiden Konzepte deutlich voneinander unterscheiden. Der Vollständigkeit halber sollten Sie aber wissen, dass für die Emulation einer anderen Plattform mit anderem Prozessor (wie beispielsweise ein PC, der eine Sony PlayStation 3 emuliert) für eine angemessene Geschwindigkeit Hardware erforderlich ist, die um Größenordnungen leistungsfähiger sein muss als die Hardware der emulierten Plattform.

22.2.3 Clientseitige Virtualisierung

Die Virtualisierung lässt sich auf vielfältige Weise nutzen und in diesem Abschnitt wollen wir uns einige Beispiele ansehen. Bevor ich fortfahre, möchte ich die Grundlagen mit einfachen Worten zusammenfassen. Bei der *clientseitigen Virtualisierung* läuft die VM auf dem lokalen Rechner (im Gegensatz zu einer VM, die anderenorts ausgeführt wird – dazu komme ich später), wobei es keine Rolle spielt, ob die eigentliche VM-Datei auf dem lokalen Rechner oder auf einem zentralen Server im Netzwerk gespeichert ist.

Im Prinzip besteht das Erstellen einer virtuellen Maschine aus folgenden Schritten:

1. Überprüfen Sie, ob die Hardware Ihres Systems Virtualisierung unterstützt, und richten Sie es gegebenenfalls dafür ein.
2. Installieren Sie einen Hypervisor auf dem System.
3. Erzeugen Sie eine virtuelle Maschine, die den Systemanforderungen des Gastbetriebssystems genügt.
4. Starten Sie die neue VM und installieren Sie das Gastbetriebssystem wie auf einem normalen, physischen Computer.

Hardwareunterstützung

Zwar unterstützen alle Computer, auf denen Linux, Windows oder macOS läuft den Betrieb eines Hypervisors, allerdings muss einigen Anforderungen an die Hardware Beachtung geschenkt werden. Der Hypervisor wird deutlich besser funktionieren, wenn Sie die Hardwareunterstützung für Virtualisierung aktivieren.

Zwar bringen seit Ende der 1980er-Jahre alle Intel-CPUs Multitaskingunterstützung für den Supervisor mit, dennoch ist es für die CPU Schwerstarbeit, mehrere Supervisors auf mehreren virtuellen Maschinen gleichzeitig zu betreiben. Seit etwa 2005 haben sowohl AMD als auch Intel ihren CPUs weitere Funktionalitäten zur besseren Unterstützung von Hypervisoren hinzugefügt: Intel stellte *VT-x* und AMD *AMD-V* vor. Hierbei handelt es sich um die sogenannte *Hardwareunterstützung der Virtualisierung*.

Falls Ihre CPU und Ihr BIOS die Hardwareunterstützung der Virtualisierung beherrschen, können Sie diese im System-Setup-Programm aktivieren. Abbildung 22.11 zeigt diese Einstellung in einem typischen System-Setup-Programm.

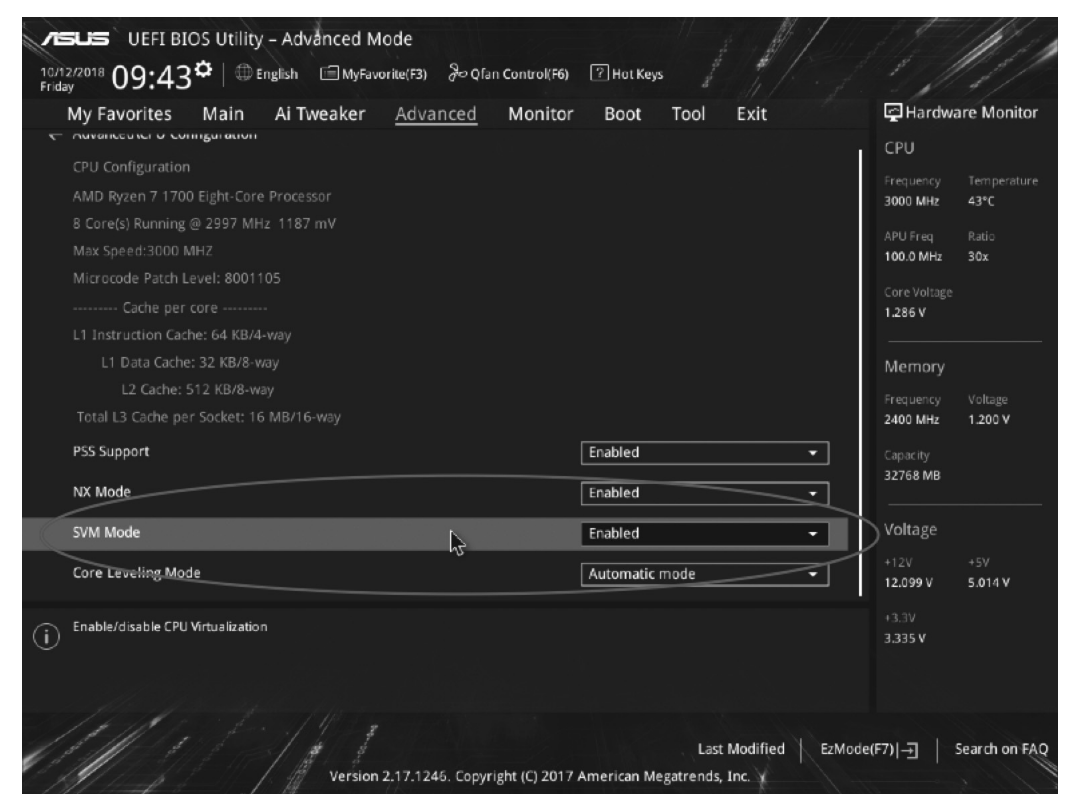


Abb. 22.11: BIOS-Einstellung zur Aktivierung der Hardwareunterstützung für Virtualisierung

RAM

Neben der Hardwareunterstützung der Virtualisierung spielt die RAM-Ausstattung die wichtigste Rolle. Jede virtuelle Maschine benötigt ebenso viel Arbeitsspeicher wie eine echte, daher ist es gängige Praxis, den Wirtscomputer mit so viel RAM wie möglich zu bestücken. Je mehr virtuelle Maschinen Sie betreiben, desto mehr RAM benötigen Sie. Im Allgemeinen sind hier zwei Punkte zu beachten:

- Lassen Sie genügend Arbeitsspeicher für den Hypervisor selbst frei.
- Bauen Sie hinreichend viel RAM ein, damit allen gleichzeitig laufenden virtuellen Maschinen eine angemessene Menge Arbeitsspeicher zur Verfügung steht.

Wie viel RAM Sie tatsächlich benötigen, müssen Sie erst einmal herausfinden. Ich betreibe einen VirtualBox-Hypervisor auf einem Rechner mit Windows 8.1 (64-Bit), der drei virtuelle Maschinen beherbergt: ein System mit Windows 7, auf dem eine Simulation läuft, ein Ubuntu-Linux (64-Bit) mit einem Webserver und ein System mit Windows 10 (64-Bit), das als Remotedesktopserver arbeitet. Die drei virtuellen Maschinen sind stets gut ausgelastet. Ich habe durch Recherchieren im Internet (und durch ein wenig Schätzen) folgenden Arbeitsspeicherbedarf ermittelt:

- 4 GB für das Wirtssystem und VirtualBox
- 1 GB für Windows 7
- 512 MB für Ubuntu
- 2,5 GB für Windows 10

Um nicht am falschen Ende zu sparen, habe ich 32 GB RAM in das System eingebaut, und es läuft bislang prächtig! Hier ist dennoch Vorsicht geboten, denn der exakte Speicherbedarf lässt sich nur schwer einschätzen. Sie kommen möglicherweise zu einem anderen Ergebnis.

Hinweis

Wie Sie aus Kapitel 4 wissen, ist die RAM-Unterstützung von Mainboards unterschiedlich. Wenn Sie vorhaben, auf einem Rechner virtuelle Maschinen zu betreiben, lohnt es sich, bei der Auswahl seine Hausaufgaben zu machen, sonst müssen Sie sich womöglich mit 16 GB RAM begnügen.

Festplattenplatz

Genügend Speicherplatz auf der Festplatte ist ebenfalls wichtig, denn die VM-Dateien können wirklich riesig sein, weil sie ja alles beinhalten, was auf der virtuellen Maschine installiert ist. Je nach Betriebssystem und Einsatzgebiet kann die Größe einer VM-Datei von einigen Megabyte bis zu Hunderten von Gigabyte reichen. Darüber hinaus belegt jeder angelegte Snapshot oder Sicherungspunkt ebenfalls Speicherplatz. Wie Sie Abbildung 22.12 entnehmen können, belegt eine virtuelle Maschine mit Windows 10 mehr als 14 GB.

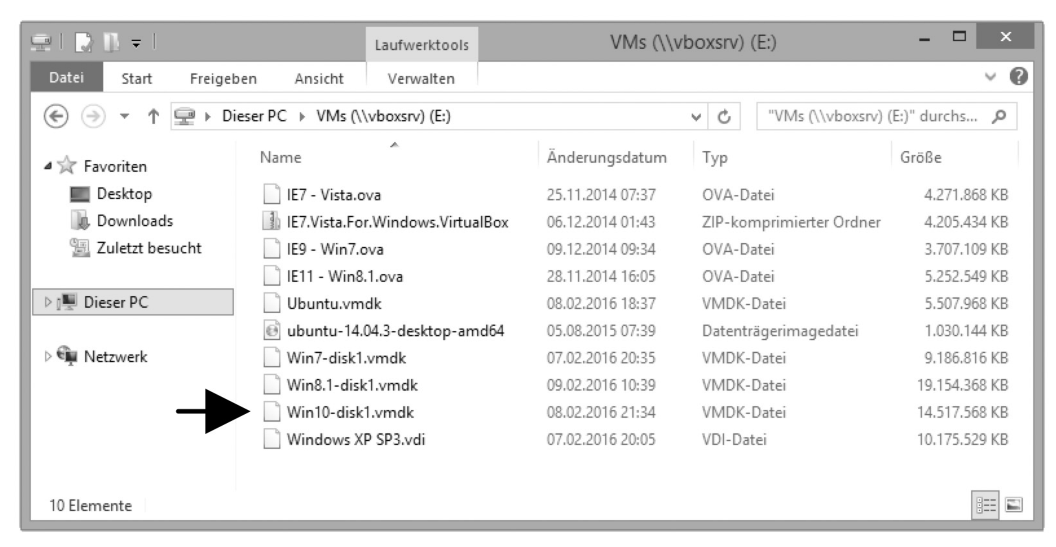


Abb. 22.12: Ordner mit VM-Dateien

Die Details hängen natürlich von den gegebenen Umständen ab, aber hier sind ein paar allgemeine Empfehlungen:

- Vergewissern Sie sich, dass ausreichend Speicherplatz für alle geplanten VMs vorhanden ist, und lassen Sie auch noch etwas Spielraum nach oben.
- Ihre VMs sind wertvoll. Schützen Sie sie durch einen RAID-Verbund und regelmäßige Backups, um zu gewährleisten, dass sie verfügbar sind, wenn sie benötigt werden.
- Wenn die Geschwindigkeit für Ihre VMs von Bedeutung ist, sollten Sie diese auf einer SATA- oder NVMe-SSD speichern.

Netzwerkunterstützung

Zu den interessantesten Features von VMs gehören die vielen Möglichkeiten, diese »virtuell« zu vernetzen. Können Sie eine VM mit dem Internet verbinden? Natürlich können Sie das, aber der Hypervisor leistet erheblich mehr. Tatsächlich kann er die virtuellen Maschinen ganz nach Bedarf auf verschiedene Weise in das Netzwerk einbinden.

Internes Netzwerk Nehmen wir an, Sie betreiben vier VMs und möchten, dass diese einander im Netzwerk »sehen« können, andere Geräte hingegen nicht. Keine Internetverbindung, sondern nur die vier VMs, die meinen sollen, die einzigen vorhandenen Computer zu sein. In diesem Fall konfigurieren Sie für alle vier VMs die virtuelle Netzwerkkarte als INTERNES NETZWERK (Abbildung 22.13). Auf diese Weise verhalten sich die VMs dieses Hypervisors so, als ob sie an einem Switch angeschlossen wären, mit dem keine weiteren Geräte verbunden sind.

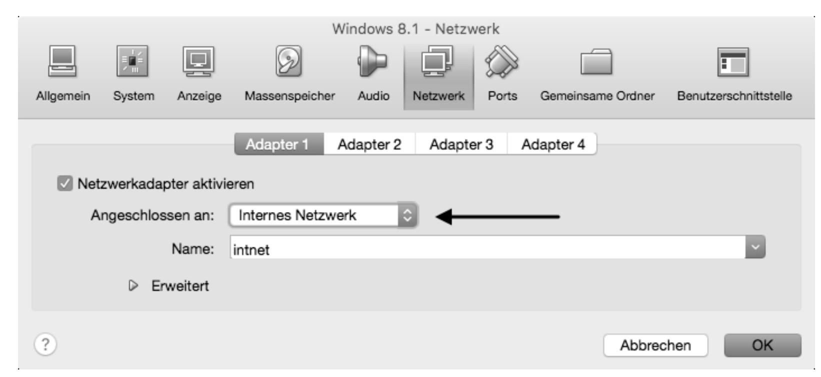


Abb. 22.13: Konfiguration des Netzwerks einer VM in VirtualBox

Die Einstellung INTERNES NETZWERK ist wirklich praktisch, wenn Sie mit irgendeinem schicken Netzwerktool herumexperimentieren möchten, ohne dabei Gefahr zu laufen, irgendeinen Schaden außerhalb Ihres kleinen virtuellen Netzwerks anzurichten. Ich stoße des Öfteren auf interessante Werkzeuge, die ich *keinesfalls* in einem produktiv genutzten Netzwerk einsetzen würde (Malware-Tools, Netzwerkscanner und dergleichen). Indem ich ein paar VMs einrichte und sie als internes Netzwerk konfiguriere, kann ich nach Herzenslust herumspielen, ohne befürchten zu müssen, das echte Netzwerk durcheinanderzubringen.

Netzwerkbrücke Die meisten Leute stellen sich beim Vernetzen einer neuen VM vor allem die Frage, wie sie sich mit dem Internet verbinden lässt. Zunächst einmal müssen sie die VM mit dem echten Netzwerk verbinden. In vielen Situationen ist es erwünscht, dass die VM auf genau dieselbe Weise mit dem Netzwerk verbunden ist wie die Wirtsmaschine. Die virtuelle Netzwerkkarte reitet sozusagen »huckepack« auf der echten Netzwerkkarte, um eine Verbindung zum Netzwerk herzustellen. (Die korrekte Bezeichnung dafür lautet *Netzwerkbrücke.*) Eine VM mit Netzwerkbrücke greift auf dasselbe Netzwerk wie die Wirtsmaschine zu. Es verhält sich ungefähr so, als ob die VM mit einem eigenen Kabel am Netzwerk angeschlossen sei. Eine Netzwerkbrücke stellt eine einfache Möglichkeit dar, die VM mit dem Internet zu verbinden – natürlich vorausgesetzt, dass die Wirtsmaschine über einen Internetzugang verfügt.

Wichtig

Über eine Netzwerkbrücke mit dem Internet verbundene VMs sind den gleichen Sicherheitsrisiken ausgesetzt wie ein echter Computer.

In der nachfolgend geschilderten Situation ist eine Netzwerkbrücke angebracht. Jemand versucht, auf meine Onlinevideos zuzugreifen, stößt dabei jedoch auf Schwierigkeiten. Um das Problem nachzu-

vollziehen, richte ich eine VM mit dem Betriebssystem und dem Browser des Kunden ein. Die Netzwerkkarte der VM würde ich dann als Netzwerkbrücke konfigurieren. Die echte Netzwerkkarte wird damit angewiesen, der virtuellen NIC den Zugriff auf das Netzwerk zu gestatten, ganz als ob sie eine echte, am selben Netzwerk angeschlossene Netzwerkkarte wäre. Sie kann dann wie eine echte Netzwerkkarte über DHCP (*Dynamic Host Configuration Protocol*) Informationen abrufen.

Wichtig

Nahezu jeder Hypervisor verwendet beim Anlegen einer neuen VM die Voreinstellung Netzwerkbrücke oder NAT (*Network Address Translation*), sofern Sie die virtuelle NIC nicht umkonfigurieren.

Virtuelle Switches Wenn Sie ein internes Netzwerk mit vier virtuellen Maschinen einrichten, müssen diese auf irgendeine Art und Weise miteinander verbunden werden. In einem echten Netzwerk sind die Computer über einen Switch miteinander verbunden. Und auch der Hypervisor kann virtuelle Switches verwenden! Dafür gibt es verschiedene Methoden. VirtualBox richtet beispielsweise automatisch virtuelle Switches ein und Sie sehen davon nichts. Microsofts Hyper-V hingegen erfordert beim Aufbau eines Netzwerks die Einrichtung virtueller Switches. Abbildung 22.14 zeigt den Manager für virtuelle Switches bei der Konfiguration eines virtuellen Switches.

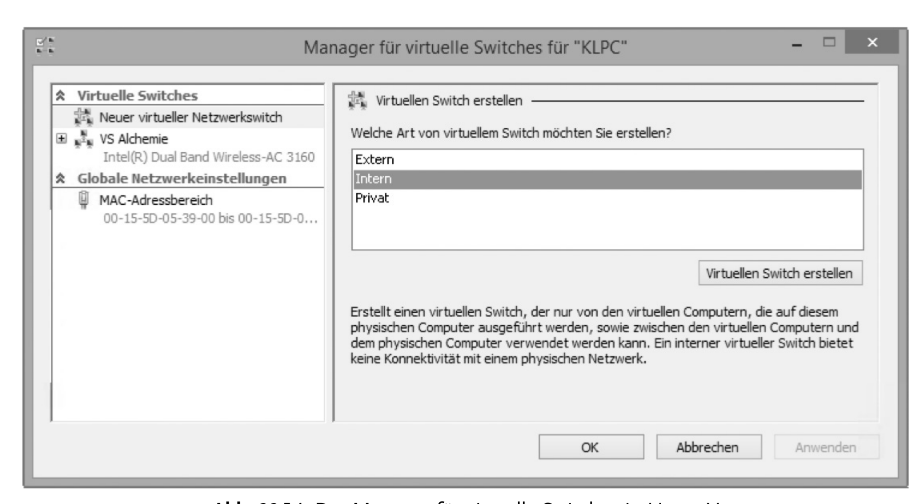


Abb. 22.14: Der Manager für virtuelle Switches in Hyper-V

Nicht angeschlossen Eine weitere Netzwerkoption ist der völlige Verzicht darauf. Zum Erzeugen einer VM ist nicht unbedingt ein Netzwerkanschluss erforderlich. Ich verwende einige VMs zum Testen von Software, die eigenständige Rechner sind. Netzwerkzugang benötige ich dafür nicht. Ich schließe einfach einen USB-Stick an, der die zu testende Software enthält und schon kann ich loslegen.

Wichtig

Den Zweck eines Hypervisors und von VMs sollten Sie kennen. Und auch clientseitige Virtualisierung, Emulation, Sicherheitsanforderungen und Netzwerkunterstützung sollten Ihnen geläufig sein.

Installation einer virtuellen Maschine

Der eigentliche Installationsvorgang des Hypervisors ist für gewöhnlich auch nicht komplizierter als die Installation anderer Software. Sehen wir uns Hyper-V als Beispiel an. Wenn Sie über einen Rechner mit Windows 8/8.1/10 verfügen, können Sie Hyper-V installieren, indem Sie im Applet PROGRAMME UND

FEATURES den Link WINDOWS-FEATURES AKTIVIEREN ODER DEAKTIVIEREN auswählen, der das Dialogfeld WINDOWS-FEATURES öffnet (Abbildung 22.15).



Abb. 22.15: Hyper-V in Windows 8.1 installieren

Nachdem Sie einen Hypervisor Ihrer Wahl aktiviert haben, steht Ihnen ein Manager für virtuelle Maschinen zur Verfügung, der als Ausgangspunkt zum Erstellen, Starten, Stoppen, Speichern und Löschen von VMs dient. Abbildung 22.16 zeigt den Oracle VirtualBox Manager.

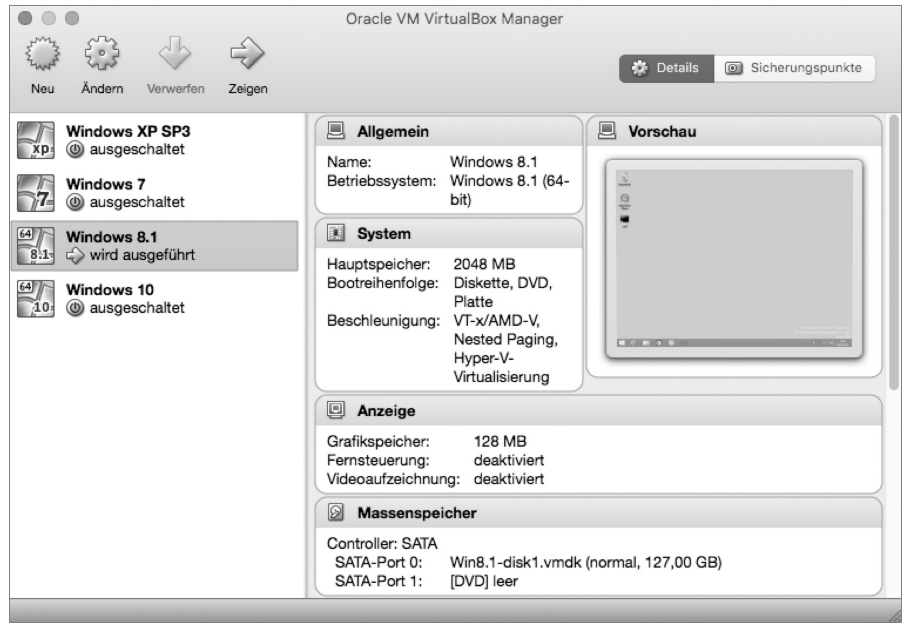


Abb. 22.16: Oracle VirtualBox Manager mit vier installierten VMs

Erstellen einer virtuellen Maschine

Nun ist es an der Zeit, eine virtuelle Maschine einzurichten. Bei praktisch jedem VM-Manager gibt es zu diesem Zweck einen Menüpunkt mit einer Bezeichnung wie NEU|VIRTUELLE MASCHINE oder MASCHINE|NEU, mit dem ein Assistent gestartet wird, der sicherstellen soll, dass Sie eine für Ihr Gastbetriebssystem geeignete VM erstellen. Meistens gibt es bereits vorkonfigurierte VMs, bei denen die wichtigsten Einstellungen Werte besitzen, die gewährleisten, dass dem Gastbetriebssystem die erforderliche virtuelle Hardware bereitsteht, um einwandfrei zu funktionieren. Abbildung 22.17 zeigt den VirtualBox-Assistenten bei der Abfrage, welches Betriebssystem installiert werden soll. Durch die Auswahl einer der Vorgaben stellen Sie sicher, dass dem Gastbetriebssystem das benötigte virtuelle RAM, der erforderliche Festplattenplatz usw. zur Verfügung stehen. Außerdem müssen Sie der virtuellen Maschine einen Namen geben. Hier wähle ich »Fedora«.

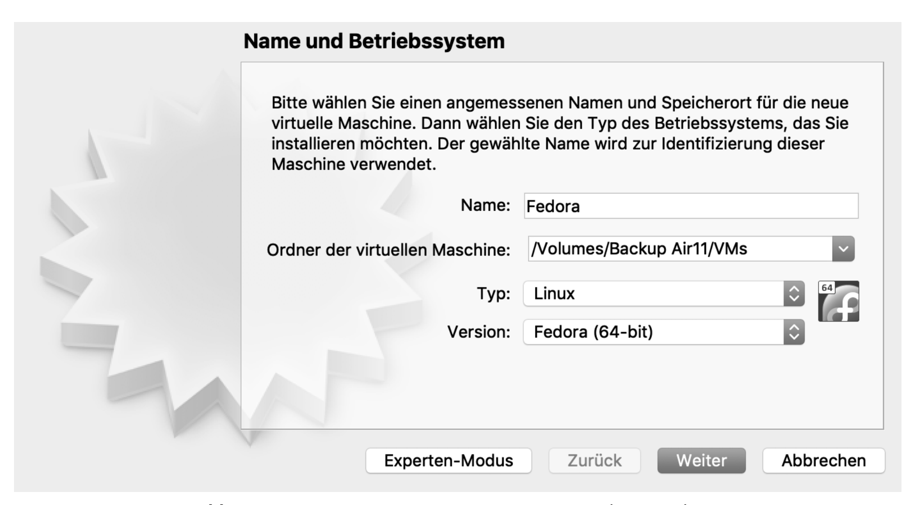


Abb. 22.17: Erzeugen einer neuen VM mit Oracle VirtualBox

Hinweis

Verwenden Sie für die Bezeichnung der VMs aussagekräftige Namen. Sie ersparen sich damit eine Menge Ärger, wenn Sie mehrere VMs auf einem Hypervisor betreiben.

Als Nächstes muss die Speichergröße angegeben werden (Abbildung 22.18). VirtualBox empfiehlt minimal 1 GB für Fedora, aber ich wähle lieber 2 GB, damit meine VM mehr RAM zur Verfügung hat. Nach dem Bestätigen der RAM-Zuweisung an die VM können Sie eine virtuelle Festplatte erzeugen. Der Assistent stellt verschiedene technische Fragen über den Typ der Festplatte, den Speicherort usw. Hier behalte ich die Voreinstellungen bei, aber es kann unter bestimmten Umständen nützlich sein, sie zu ändern. Abschließend muss angegeben werden, wie groß die Festplatte sein soll. Voreingestellt sind 8 GB, aber das ist mir zu wenig, deshalb stelle ich 25 GB ein (Abbildung 22.19). Mit diesen Einstellungen wird nun eine virtuelle Maschine erzeugt.



Abb. 22.18: Auswahl der Speichergröße



Abb. 22.19: Größe der Festplatte einstellen

Installieren des Betriebssystems

Nun ist die neue VM eingerichtet und das Betriebssystem soll installiert werden. Glauben Sie nicht, dass bei einer virtuellen Maschine Betriebssystem und Programme nicht real sind. Sie müssen auch auf einer virtuellen Maschine ein Betriebssystem installieren. Das geschieht genau so wie bei einem echten Computer dadurch, dass Sie eine CD oder eine DVD verwenden. Sie können auch Windows selbst als virtuelle Maschine betreiben, sollten aber berücksichtigen, dass für jede Windows-Kopie eine eigene Lizenz erforderlich ist. Gleiches gilt für auf der VM installierte lizenzierte Software.

Nach dem Start der neu erstellten VM fordert der Hypervisor Sie auf, ein Installationsmedium auszuwählen. Da virtuelle Maschinen hinsichtlich der Hardware so flexibel sind, können Sie das optische Laufwerk des Wirtssystems, einen USB-Stick oder auch eine ISO-Datei zur Installation eines Betriebssystems verwenden. Ich installiere hier Fedora und habe mir zu diesem Zweck ein ISO-Image von der Fedora-Website (`http://getfedora.org`) heruntergeladen, das ich zur Installation ausgewählt habe (Abbildung 22.20).

Nachdem Sie all diese Konfigurationsbildschirme hinter sich gelassen haben, können Sie die VM verwenden. Sie können sie starten, stoppen oder pausieren und virtuelle Hardware hinzufügen oder entfernen und die VM wie einen echten Computer verwenden. Abbildung 22.21 zeigt den VirtualBox-Manager mit der neu installierten VM, die hier ausgeschaltet ist.

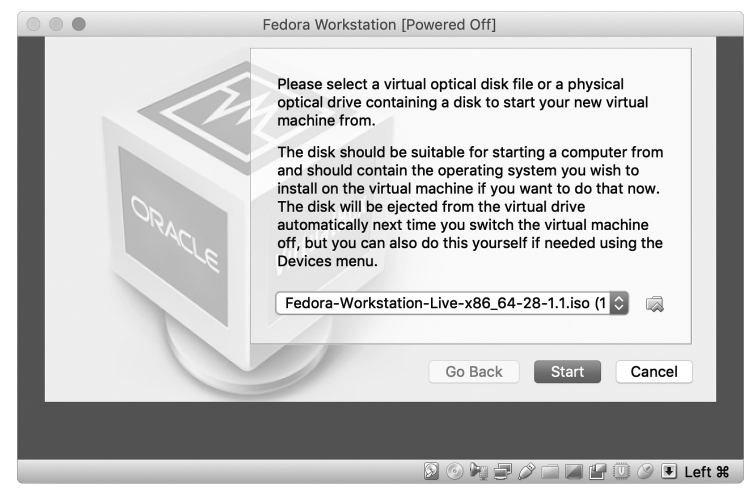


Abb. 22.20: Auswahl des Installationsmediums

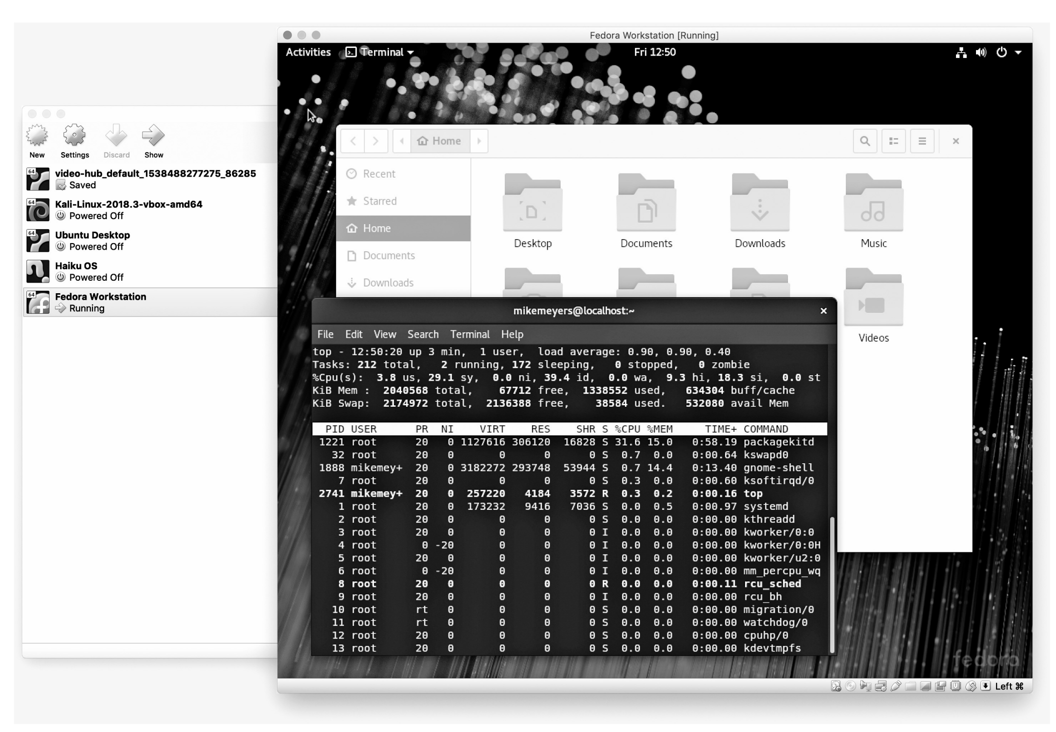


Abb. 22.21: VirtualBox mit neu installierter VM

Glückwunsch! Sie haben soeben einen *virtuellen Desktop* eingerichtet. Wie bei einem echten System können Sie Hardware entfernen oder hinzufügen – und dazu müssen Sie noch nicht einmal ein Elektronikgeschäft aufsuchen. Die eigentliche Stärke eines Hypervisors ist die Flexibilität der virtuellen Hardware. Der Hypervisor muss die Ein- und Ausgaben verarbeiten bzw. liefern können, die das Betriebssystem von normaler Hardware erwartet. Ein vernünftiger Hypervisor erlaubt es, virtuelle Festplatten, virtuelle Netzwerkkarten, virtuellen Arbeitsspeicher usw. hinzuzufügen oder zu entfernen

und ermöglicht es Ihnen auf diese Weise, den virtuellen Desktop an Ihre Bedürfnisse anzupassen. Abbildung 22.22 zeigt einige der Einstellungsmöglichkeiten in VirtualBox.

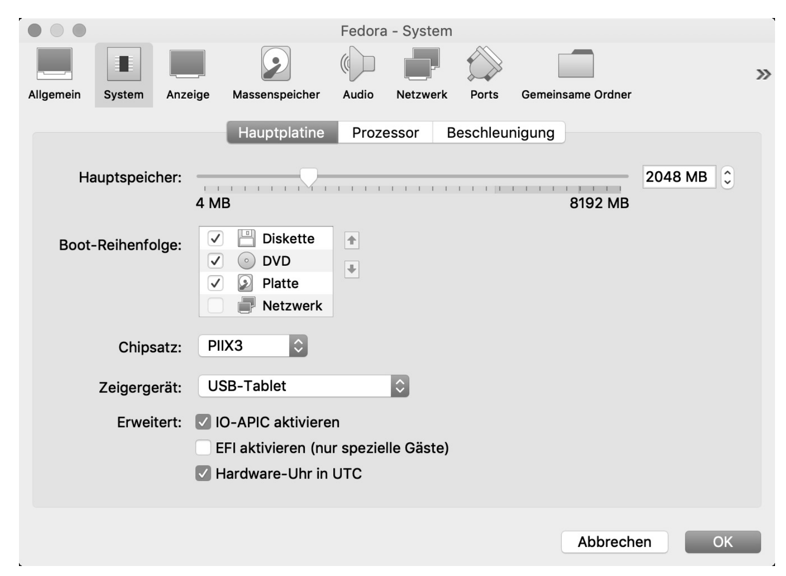


Abb. 22.22: Konfiguration der virtuellen Hardware in VirtualBox

Tipp

Sehen Sie sich die Übungen zu Kapitel 22 zum Thema »Virtuelle Hardware« unter `http://totalsem.com/100x` an! Sie können damit Ihr Verständnis der Terminologie und die Kenntnisse der Schritte bei der Einrichtung einer VM vertiefen.

22.2.4 Serverseitige Virtualisierung

Wenn es um Serversysteme geht, hat die Virtualisierung praktisch überall Einzug gehalten. Viele der Server, auf die wir zugreifen, insbesondere Web- und E-Mail-Server, sind jetzt virtualisiert. Wie bei allen verbreiteten Technologien arbeiten viele Menschen kontinuierlich daran, die Virtualisierung weiter zu verbessern. Das vorhin erwähnte Beispiel VMware Workstation ist eine äußerst leistungsfähige Desktop-Anwendung, wird jedoch innerhalb des Betriebssystems ausgeführt – dem Wirtsbetriebssystem.

Könnte man nicht die Leistung verbessern, indem man vollständig auf das Betriebssystem verzichtet und ausschließlich einen Hypervisor installiert? Das ist tatsächlich möglich! Dazu wird eine leistungsfähige Kombination aus Hypervisor und Betriebssystem eingesetzt, die auch *Hypervisor des Typs 1* genannt wird. Hier gibt es zwischen Hypervisor und Gastbetriebssystem keine weitere Softwareebene. Anwendungen wie VMware Workstation oder VirtualBox werden hingegen als *Hypervisor des Typs 2* bezeichnet (Abbildung 22.23).

2001 hat VMware *ESX* vorgestellt, einen Hypervisor des Typs 1, der sich des überflüssigen Verwaltungsaufwands eines Wirtsbetriebssystems entledigte, um dieses Ziel zu erreichen. ESX ist in VMwares Produktlinie zwischenzeitlich durch ESXi abgelöst worden. Dieser Hypervisor ist so leistungsfähig ist, dass er das sonst benötigte Wirtsbetriebssystem vollständig ersetzen kann und aus dem Rechner ein Gerät macht, das ausschließlich virtuelle Maschinen unterstützt. Von ESXi selber ist nicht viel zu sehen; es handelt sich schlicht um ein kleines Betriebssystem, das häufig auf einem anderen Gerät als der Festplatte installiert ist, z.B. auf einem USB-Stick. Tatsächlich werden die VMs nicht auf dem ESXi-Server selbst verwaltet, weil so ziemlich alles über eine Webschnittstelle erledigt wird (Abbildung 22.24).

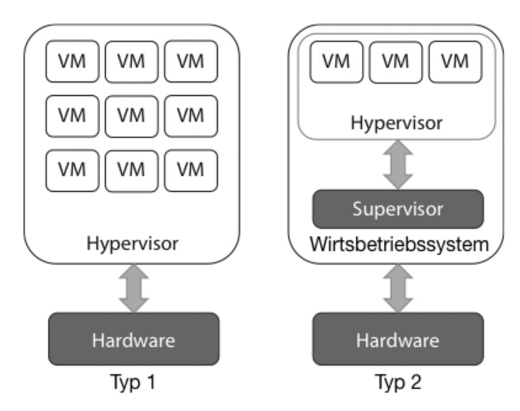


Abb. 22.23: Hypervisor des Typs 1 und des Typs 2

totalvm.totalhome

Welcome to VMware ESXi 5.1

VMware ESXi 5.1
Welcome

Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

- Download vSphere Client

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- Download VMware vCenter

If you need more help, please refer to our documentation library:

- vSphere Documentation

You are running Dell Customized Image ESXi 5.1.0 A01(based on ESXi 5.1.0 VMKernel Release Build 799733)

- Click here to visit support.dell.com

For Administrators

vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- Download the Virtual Appliance
- Download the Windows Installer (exe)
- Download the Linux Installer (tar.gz)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- Browse datastores in this host's inventory

For Developers

vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- Learn more about the Web Services SDK
- Browse objects managed by this host

Copyright © 1998-2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware products may contain individual open source software components, each of which has its own copyright and applicable license conditions. Please visit http://www.vmware.com/info?id=1127 for more information.

Abb. 22.24: Die Webschnittstelle von ESXi

Ein Server, dessen Hypervisor sich auf einem USB-Stick befindet, kann den gesamten Festplattenplatz zum Speichern von VMs nutzen oder sogar ganz auf Festplatten verzichten und die VMs in einem SAN (*Storage Area Network*) ablegen. Das verbessert die Leistung, und weil sich alle Laufwerke am selben Ort befinden, wird Wartung, Administration und Backup der Laufwerke vereinfacht. In Abbildung 22.24 ist erkennbar, wie meine ESXi-Version geladen wird: von einem USB-Speicherstick. Nach dem Einschalten des Servers wird ESXi vom USB-Stick gestartet und kurz danach erscheint eine rudimentäre Schnittstelle, in der sich grundlegende Informationen wie das Kennwort und eine statische IP-Adresse eingeben lassen.

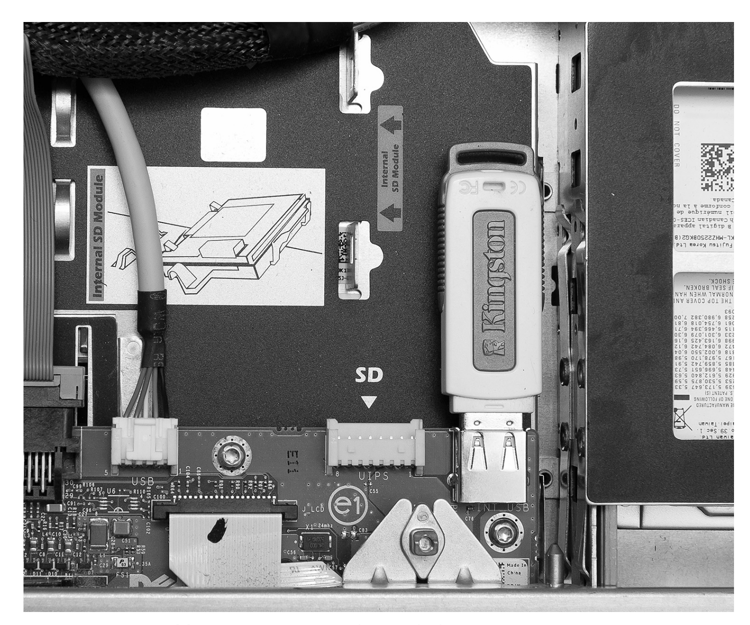


Abb. 22.25: USB-Speicherstick des Serversystems

Lassen Sie sich von der geringen Größe des ESXi-Hypervisors nicht in die Irre führen. Das Betriebssystem ist so klein, weil es nur eine einzige Aufgabe zu erfüllen hat: als Wirt für virtuelle Maschinen zu dienen. Es handelt sich um außerordentlich mächtige Software.

Um die Bedeutung der Virtualisierung wirklich zu verstehen, muss man sich vergegenwärtigen, wie auch die Flexibilität steigt, wenn der Umfang der zu erledigenden Aufgaben wächst. Betrachten wir das Ganze einmal aus einer anderen Perspektive und reden über Geld. Dank des Geldes verfügen wir über einheitliche, leicht unterteilbare Währungseinheiten, die wir gegen Güter und Dienstleistungen eintauschen können. Ohne Geld wären wir auf einen reinen Tauschhandel angewiesen, und bevor es Geld gab, wurden Güter und Dienstleistungen auch direkt ausgetauscht.

Nehmen wir an, ich sei kurz vorm Verhungern und besitze lediglich einen Hammer. Sie hingegen haben ein Hühnchen, das ich gerne hätte. Also biete ich Ihnen an, mit meinem Hammer irgendetwas für Sie herzustellen. Eigentlich sind Sie aber nur an einem eigenen Hammer interessiert. Auf den ersten Blick sieht das wie ein perfekter Tauschhandel aus. Doch wenn mein Hammer nun tatsächlich mindestens fünf Hühnchen wert ist, was dann? Ich kann Ihnen schließlich nicht ein Fünftel meines Hammers geben, und wenn ich ihn gegen Ihr Hühnchen tausche, fehlt mir das Werkzeug, um irgendetwas anderes herzustellen. Ich habe nur die Wahl, entweder auf das Hühnchen zu verzichten oder aber meinen Hammer weit unter Wert herzugeben. Wäre mein Hammer doch nur Geld!

Und nun zu Mario, der zwei physische Server betreibt. Im Grunde genommen hat er also zwei wirklich sehr teure Hämmer. Wenn er einen davon verwendet, um eine kleine, aber unverzichtbare Website zu betreiben, geht ein Großteil des Leistungspotenzials dieses Servers verloren (zumal sie wohl kaum auf

der Startseite von `reddit.com` landen wird). Wenn Mario nun einen Hypervisor auf seinen Servern installiert, wäre das ein großer Schritt nach vorn, denn er könnte sie nun viel produktiver nutzen.

Hinweis

Falls Sie es noch nicht kennen: Reddit ist ein bemerkenswerter Treffpunkt für Geeks im Internet. Besuchen Sie das CompTIA-Forum unter `http://www.reddit.com` und sagen Sie Hallo. Sie finden dort eine Fülle von Informationen über CompTIA A+ und andere Zertifizierungen.

Marios Server ähneln nun weniger Hämmern, sondern eher einer Währung oder Geld. Ich kann nach wie vor nicht ein Fünftel meines Hammers eintauschen, aber Mario kann problemlos eine VM für seine Website einrichten, die nur ein Fünftel (oder irgendeinen anderen Bruchteil) der Ressourcen seines Servers in Anspruch nimmt. Wenn er weitere Server hinzufügt, kann er die verfügbaren Ressourcen leicht in Einheiten unterteilen. Jeder neue Server erweitert die Ressourcen, und wenn Mario allmählich weitere VMs mit unterschiedlichem Ressourcenbedarf hinzufügt, steigt auch die Anzahl der Möglichkeiten, sie auf die verschiedenen Server zu verteilen, um die ungenutzten Ressourcen zu minimieren (Abbildung 22.26).

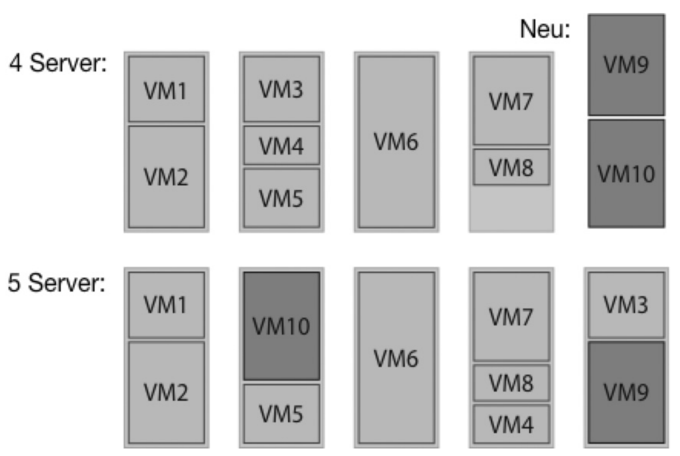


Abb. 22.26: Hier werden keine Ressourcen verschwendet.

22.3 Cloud Computing

Die einfache Virtualisierung ermöglicht es Mario zwar, die Ressourcennutzung (wie im vorhergehenden Abschnitt beschrieben) zu optimieren, wenn sein Bedarf an Rechenkapazität und Speicherplatz wächst, er ist dabei aber auf die Leistungsfähigkeit seiner lokalen Hardware beschränkt. Erfreulicherweise ist er aber nicht länger nur auf die eigene Hardware angewiesen. Da es sich bei seinen virtuellen Maschinen lediglich um auf einem Hypervisor laufende Dateien handelt, kann er sie auch in der *Cloud* betreiben, in einem weltweiten Netzwerk von Servern.

Denken Sie an den Betrieb eines einfachen Webservers. Vor nicht allzu langer Zeit war es erforderlich, ein System einzurichten, einen Webserver zu installieren, einen Internetzugang mit entsprechender Bandbreite zu beauftragen, dem korrekt konfigurierten Rechner eine öffentliche IP-Adresse zuzuweisen, eine Firewall einzurichten und das System zu administrieren. Die Kosten für die Einrichtung betrugen mehrere Tausend Euro und der Betrieb schlug mit weiteren hundert Euro oder mehr im Monat zu Buche. Und nicht auszudenken, wenn das System einmal ausfiel!

Im Laufe der Zeit traten dann Webhosting-Dienste in Erscheinung, die Ihnen einen Großteil der mit der Einrichtung einer Serverinfrastruktur einhergehenden Arbeiten abnahmen. Sie bekamen Spei-

cherplatz auf einem Server bereitgestellt, der auch andere Websites beherbergte. Dadurch konnten Sie sich die Einrichtung einer eigenen Serverinfrastruktur sparen, aber diese Dienste waren immer noch ziemlich teuer.

Circa 2005/2006 brachten verschiedene Unternehmen, allen voran Amazon, eine neue Art des Webhostings auf den Markt. Amazon stellte fest, dass die erwünschten Dienste statt von individuellen physischen Computern oder öffentlich zugänglichen Verzeichnissen auch durch große Gruppen virtualisierter Server bereitgestellt werden können, auf die man über eine leistungsfähige Benutzerschnittstelle zugreift. Die Benutzer können mit wenigen Mausklicks den Server für einen Dienst starten, den sie anbieten möchten. Das *Cloud-Computing* hatte das Licht der Welt erblickt!

Wenn ich von der Cloud spreche, meine ich damit nicht nur Filehosting-Dienste wie Dropbox oder Google Drive, sondern auch einfache Schnittstellen zu einer Vielzahl von bei Bedarf abrufbarer Computing-Ressourcen, die Amazon (Abbildung 22.27), Microsoft und viele andere Unternehmen im öffentlich zugänglichen Internet anbieten. Die Technologie, die all diesen innovativen Diensten zugrunde liegt, ist die Virtualisierung.

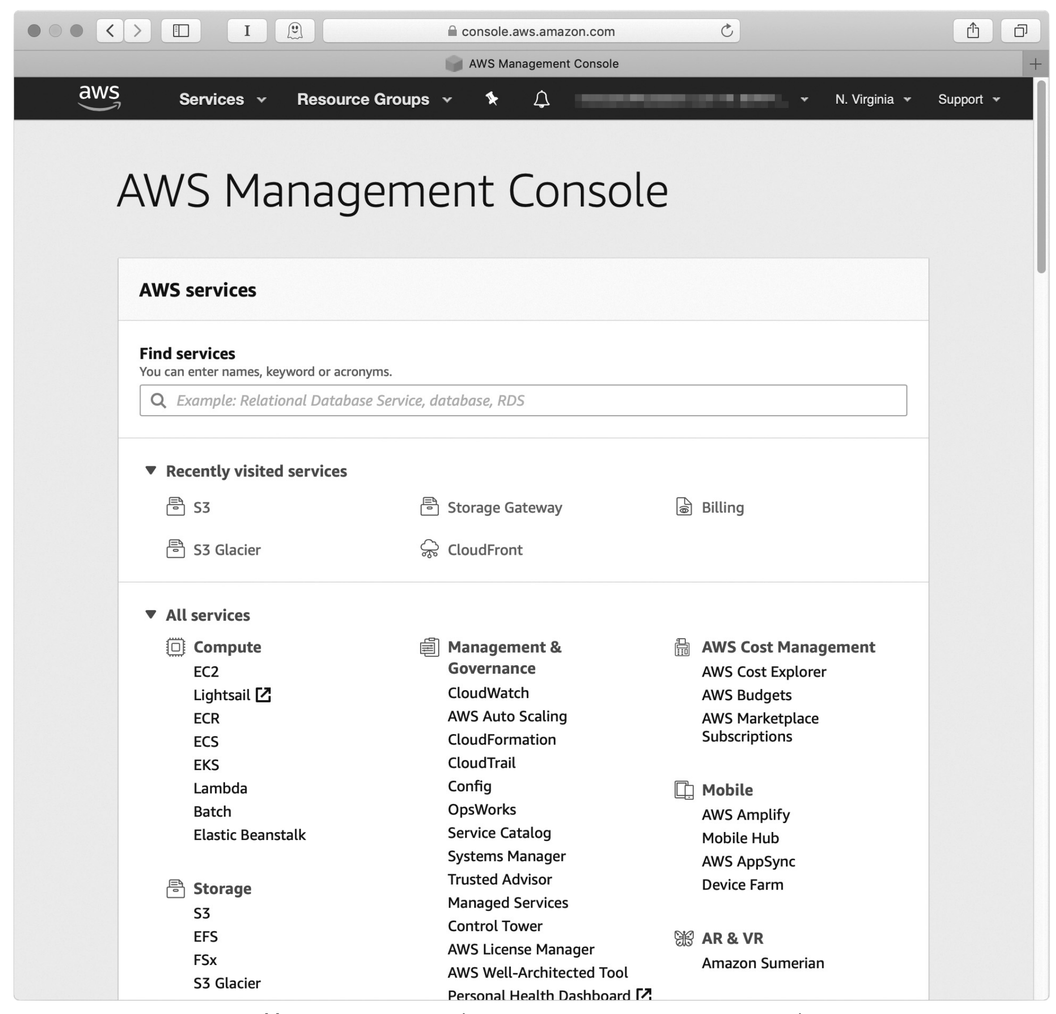


Abb. 22.27: Amazon Web Services (AWS) Management Console

22.3.1 Dienstebenen

Zum Verständnis der Cloud sind die Dienste entscheidend. Auf Hardwareebene bemerken wir gar keinen Unterschied zwischen der Cloud und den Servern und Netzwerken, aus denen das Internet als Ganzes besteht. Wir greifen auf die Server und Netzwerke der Cloud durch verschiedene Software zu, die es vereinfacht, komplexe Aufgaben zu erledigen und leistungsfähige Ressourcen zu verwalten und so der zugrunde liegenden Hardware größeren Nutzen verleiht. Als Endanwender bekommen wir nur die hübsche Oberfläche der Dienstebenen zu Gesicht – Webanwendungen wie Dropbox, Gmail oder Facebook, die als Benutzerschnittstelle fungieren. Der Rest dieser mehrschichtigen Torte von Dienstebenen dient vornehmlich dazu, solche Webanwendungen und deren Entwickler zu unterstützen. Schneiden wir diese Torte also an (Abbildung 22.28) und betrachten sie von Grund auf.

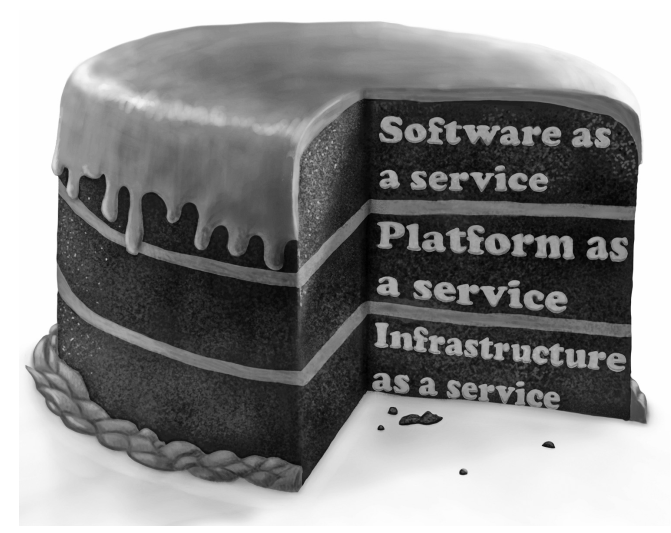


Abb. 22.28: Die mehrschichtige Torte von Dienstebenen

Infrastructure as a Service (IaaS)

Auf ähnliche Weise wie Mario in seinem lokalen Netzwerk bestmöglichen Gebrauch von seiner Hardware macht, setzen die Anbieter global verfügbarer Dienste, die als *Infrastructure as a Service* (*IaaS*) bezeichnet werden, Virtualisierung ein, um ihre Hardware so gut wie möglich auszulasten, sich vor Datenverlust und Ausfallzeiten zu schützen sowie auf höhere Belastungen zu Stoßzeiten reagieren zu können. Mario kann also auf einen IaaS-Anbieter wie Amazon Web Services (AWS) zugreifen, um bei Bedarf neue virtuelle Server mit einem Betriebssystem seiner Wahl einzurichten (Abbildung 22.29), die nur wenige Cent pro Stunde kosten. Das Schöne daran ist, dass Sie keine teure, schwere Hardware mehr kaufen müssen. Sie nutzen stattdessen Amazons leistungsfähige Infrastruktur.

Viele Websites sind im Grunde genommen Web*anwendungen*. Wenn Sie beispielsweise auf Mike Meyers Videos zugreifen möchten, besuchen Sie `http://hub.totalsem.com`. Diese Website ist eigentlich eine Anwendung, die Sie zum Betrachten von Videos, dem Üben von Prüfungsfragen usw. verwenden. Diese Webanwendung ist ein praktisches Werkzeug, aber wenn viele Leute gleichzeitig darauf zugreifen, müssen wir des Öfteren die Kapazität erhöhen, damit Sie sich nicht bei uns über einen langsamen Server beklagen. Glücklicherweise ist die Webanwendung dafür ausgelegt, auf mehreren verteilten Servern laufen zu können. Wenn wir mehr Leistung benötigen, fügen wir einfach so viele virtuelle Server hinzu wie nötig. Aber damit kratze ich nur an der Oberfläche dessen, was möglich ist. AWS biete eine Vielzahl von Diensten, die zum Betrieb komplexer Webanwendungen erforderlich sind – fast unbegrenzten Speicherplatz (Abbildung 22.30), Datenbankserver, Caching, Bereitstellung von Mediendateien und vieles mehr. Kosten fallen dabei nur entsprechend der Nutzung an.

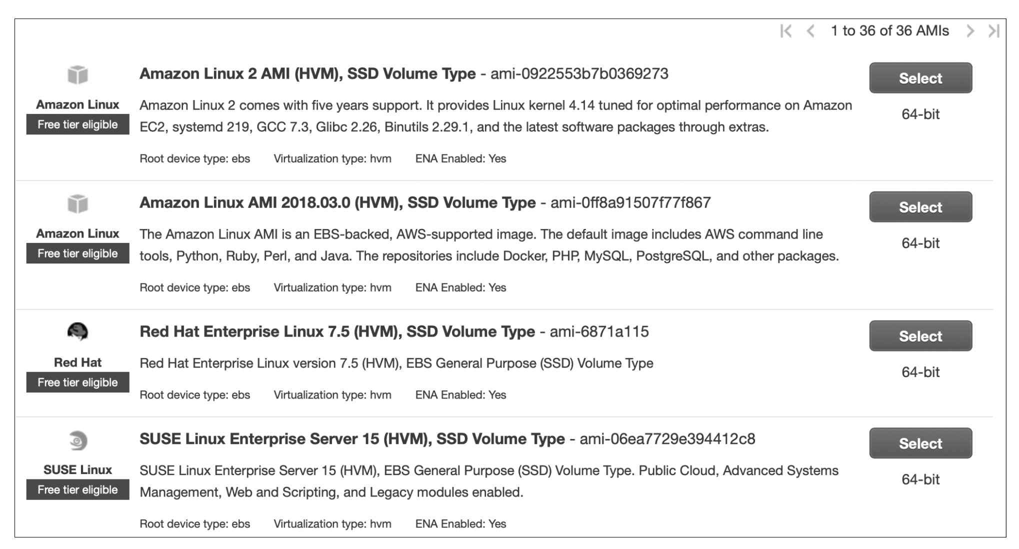


Abb. 22.29: Erstellen einer AWS-Instanz

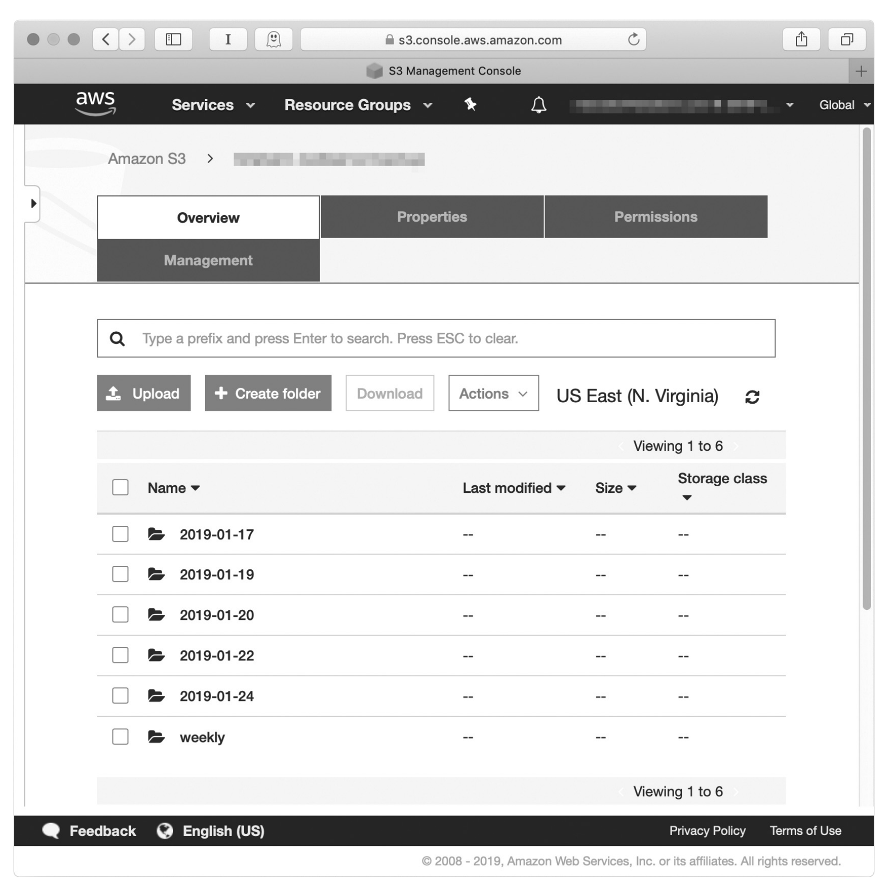


Abb. 22.30: Amazon Simple Storage Service (S3)

Der Haken dabei ist, dass man zwar nicht mehr für die Hardware verantwortlich ist, sehr wohl aber für die Konfiguration und Wartung des Betriebssystems und der Software der erstellten virtuellen Maschinen. Das bedeutet einerseits, dass man bei der Einrichtung sehr flexibel ist, andererseits sind dazu Kenntnisse des jeweiligen Betriebssystems erforderlich – und Zeit kostet es auch. Wenn Sie sich nicht selbst um die Infrastruktur, das Betriebssystem und alles andere (natürlich von der eigentlichen Anwendung abgesehen) kümmern wollen, müssen Sie sich in den Dienstebenen eine Etage höher begeben und *Platform as a Service* (*PaaS*) in Anspruch nehmen.

Platform as a Service (PaaS)

Webanwendungen werden von Programmierern erstellt. Und eins können Programmierer wirklich gut: programmieren. Das Problem dabei ist nur, dass zu einer Webanwendung sehr viel mehr gehört als nur Programmierer. Bei der Entwicklung einer Webanwendung muss die gesamte Infrastruktur gehandhabt werden: Es werden Systemadministratoren und Datenbankadministratoren benötigt, es muss allgemeinen Support für das Netzwerk geben usw. Für eine Webanwendung sind außerdem mehr als nur Hardware und ein Betriebssystem erforderlich. Man braucht auch Entwicklungswerkzeuge, Tools zur Überwachung, Software zur Verwaltung von Datenbanken und potenziell Hunderte weitere Dienste oder Hilfsprogramme. Eine Webanwendung zu entwickeln und zum Laufen zu bringen ist wahrlich keine einfache Aufgabe.

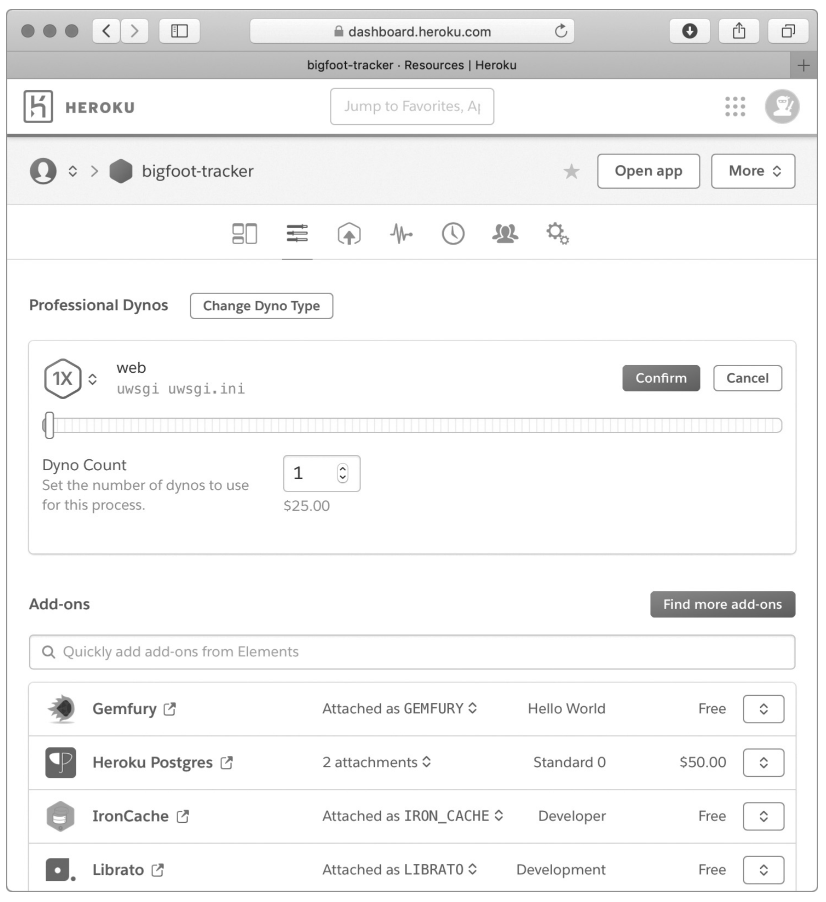


Abb. 22.31: Herokus Verwaltungskonsole

Die Anbieter von *Platform as a Service* (*PaaS*) stellt den Programmierern alle nötigen Werkzeuge zu Verfügung, die sie zum Bereitstellen, Administrieren und Warten einer Webanwendung benötigen. Der PaaS-Anbieter ermöglicht zunächst den Zugang zu irgendeiner Form von Infrastruktur, die auch von einem IaaS-Anbieter stammen kann, auf der wiederum eine Plattform aufbaut: ein komplettes System zur Handhabung der Bereitstellung, der Verwaltung und aller anderen Aspekte einer Webanwendung.

Das entscheidende Merkmal von PaaS ist, dass die der Plattform zugrunde liegende Infrastruktur für die Entwickler so gut wie unsichtbar ist. Der PaaS-Anbieter ist für die Infrastruktur verantwortlich, die Entwickler hingegen können diese nicht direkt beeinflussen und müssen sich keine Gedanken um deren Komplexität machen. Für die Entwickler ist PaaS lediglich der Ort, an dem sie ihre Anwendung platzieren und laufen lassen können.

Heroku, einer der ersten PaaS-Anbieter, hat eine einfache Schnittstelle entwickelt, die auf den IaaS-Angeboten von AWS aufbaut und die Entwicklung und Skalierung von Webanwendungen weiter vereinfacht. Herokus Verwaltungskonsole (Abbildung 22.31) ermöglicht es Entwicklern, die Leistungsfähigkeit einer Anwendung mit einem einfachen Schieberegler zu erhöhen oder zu verringern, Datenbanken hinzuzufügen, Protokolle oder Leistung zu überwachen und vieles mehr. Ein Techniker oder Entwickler, der mit der Software und den Diensten zum Installieren, Konfigurieren und Einbinden dieser Dienste in eine laufende Anwendung nicht vertraut ist, würde dafür tagelang brauchen. PaaS-Anbieter verkürzen diesen Vorgang auf ein paar Stunden oder Minuten.

Software as a Service

Software as a Service (*SaaS*) befindet sich am oberen Ende der Torte. SaaS manifestiert sich auf verschiedene Weise, aber das beste Beispiel sind die erwähnten Webanwendungen, die ich soeben erörtert habe. Manche Webanwendungen, wie z.B. das *Total Seminars Training Hub*, verlangen für die Nutzung Geld. Andere, wie Google Maps, werden kostenlos angeboten. Die Anwender dieser Software »besitzen« sie nicht; es gibt keine Installations-DVD, und Sie können auch nichts herunterladen und dauerhaft nutzen. Wenn Sie eine Webanwendung verwenden möchten, müssen Sie sich mit dem Internet verbinden und die entsprechende Website aufsuchen. Auf den ersten Blick sieht das nach einem Nachteil aus, aber andererseits bietet das SaaS-Modell bei vorhandenem Internetzugang Zugriff auf wichtige Anwendungen, ohne dass Sie Daten mitführen oder regelmäßig Softwareaktualisierungen durchführen müssen. Im Unternehmensumfeld erleichtert das Abo-Modell der SaaS-Anbieter die Finanzplanung und Hunderte oder Tausende von Rechnern greifen stets auf die aktuellste Software zu (Abbildung 22.32).

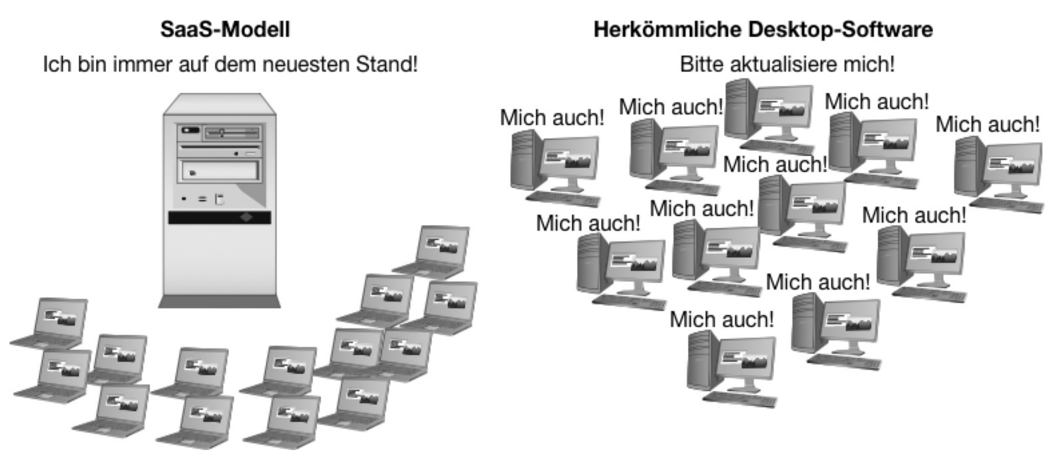


Abb. 22.32: SaaS und herkömmliche Desktops

Es ist gar nicht so einfach, SaaS exakt zu definieren, zumal man argumentieren kann, dass im Grunde genommen alles, auf das man über das Internet zugreift, in die Kategorie SaaS fällt. Vor zehn Jahren hätten wir eine Suchmaschine wie Google als Website bezeichnet, allerdings stellt sie einen Dienst bereit (die Suche), den Sie nicht Ihr Eigen nennen können, und Sie benötigen einen Internetzugang, um ihn zu verwenden. So gesehen nutzen Sie immer SaaS, wenn Sie im Internet surfen.

Dessen ungeachtet ist nicht alles eitel Sonnenschein. Wenn Sie die Flexibilität öffentlich zugänglicher SaaS-Dienste nutzen, müssen Sie im Gegenzug oft die strikte Kontrolle über Ihre Daten aufgeben. Wenn jemand Google Drive benutzt, um Entwürfe für einen Blogkommentar zu speichern, spielen Sicherheitsbedenken wohl kaum eine Rolle. Viele Unternehmen machen sich allerdings Sorgen, dass geschütztes geistiges Eigentum oder Geschäftsgeheimnisse durch nicht vertrauenswürdige Netzwerke geleitet und auf Servern gespeichert werden, die nicht unter ihrer Kontrolle stehen.

Wichtig

Die Unterschiede zwischen grundlegenden Cloud-Konzepten wie SaaS, IaaS und PaaS sollten Sie kennen.

22.3.2 Dateneigentum und Zugriff

Sicherheitsbedenken wie die eben erwähnten bedeuten nicht, dass Unternehmen auf sämtliche Vorteile des Cloud-Computings verzichten müssen. Allerdings machen sich die Unternehmensleitungen durchaus Gedanken über die Kompromisse, die bei Kosten, Kontrolle, Anpassungsfähigkeit und Privatsphäre eingegangen werden müssen. Manche Unternehmen haben darüber hinaus Ansprüche an Kapazität und Geschwindigkeit oder andere Anforderungen, denen kein Cloud-Anbieter gerecht werden kann. Über die einzugehenden Kompromisse entscheiden die Unternehmen selbst, aber für gewöhnlich ergeben sich daraus Cloud-Netzwerke, die als Public Cloud, Private Cloud, Community Cloud oder Hybrid Cloud bezeichnet werden.

Public Cloud

Die meisten Leute nutzen die *Public Cloud*, die Software, Plattformen und Infrastrukturen umfasst, die durch der allgemeinen Öffentlichkeit zugängliche Netzwerke bereitgestellt werden. Sie ist gemeint, wenn wir den Begriff *die Cloud* verwenden. Im öffentlich zugänglichen Internet können Cloud-Dienste und Anwendungen auf eine Weise miteinander zusammenarbeiten, die es erleichtert, sich deren Gesamtheit als *die Cloud* vorzustellen, anstatt an viele einzelne Public Clouds zu denken. Diese Cloud ist kein Eigentum der Öffentlichkeit – die Hardware gehört häufig Unternehmen wie Amazon, Google oder Microsoft. Aber nichts hält eine Firma wie Netflix davon ab, mit seinen Webanwendungen auf die IaaS-Angebote aller drei Anbieter gleichzeitig zurückzugreifen.

In der Public Cloud kommen alle XaaS-Varianten vor, die namensgebend für die folgenden *Cloud-Konzepte* waren:

- Public IaaS
- Public PaaS
- Public SaaS

Private Cloud

Wenn ein Unternehmen die Flexibilität der Cloud nutzen möchte, aber vollständige Kontrolle über die Daten besitzen muss und über die finanziellen Mittel verfügt, kann es eine interne Cloud einrichten, die sich im Eigentum des Unternehmens befindet – eine *Private Cloud*. Ein sicherheitsbewusstes Unternehmen könnte beispielsweise im internen Datencenter vor Ort ein IaaS-Netzwerk einrichten. Die verschiedenen Abteilungen des Unternehmens könnten ganz nach Bedarf virtuelle Maschinen erstellen oder entfernen und SaaS entwickeln, um den Bedarf an Zusammenarbeit, Planung oder Aufgaben- und Zeitverwaltung zu decken, ohne dass die Daten durch das öffentliche Internet geleitet wer-

den. Ein Unternehmen mit solchen Anforderungen, dem der Platz oder das Wissen fehlt, eine Private Cloud selbst einzurichten und zu betreiben, könnte auch einen Dienstleister beauftragen, diese Aufgaben zu übernehmen.

Auch hier gibt es private Varianten der drei Cloud-Konzepte:

- Private IaaS
- Private PaaS
- Private SaaS

Community Cloud

Mit dem englischen Begriff *Community* ist für gewöhnlich eine Gruppe von Menschen gemeint, die ein gemeinsames Ziel verfolgen oder gemeinsame Interessen pflegen. Eine *Community Cloud* hingegen ähnelt eher einer kostenpflichtigen Private Cloud und wird von mehreren Unternehmen oder Organisationen verwendet. Community Clouds werden nicht von öffentlichen oder staatlichen Stellen zum Nutzen der Bürger betrieben; die Community ist in diesem Fall eine Gruppe von Unternehmen oder Organisationen mit ähnlichen Zielen und Bedürfnissen. Stellen Sie sich vor, Sie sind Auftragnehmer des Militärs und arbeiten an einem als streng geheim eingestuften Projekt. Wäre es dann nicht praktisch, wenn Sie bei der schwierigen Aufgabe, Ihre Cloud vor von anderen Staaten finanziell unterstützten gerissenen Angreifern zu schützen, Hilfe von anderen Auftragnehmern des Militärs und der Sicherheitsdienste erhielten?

Wie bei Public und Private Cloud gibt es hier ebenfalls drei Varianten:

- Community IaaS
- Community PaaS
- Community SaaS

Hybrid Cloud

In manchen Fällen ist es tatsächlich möglich, sich den Pelz zu waschen, ohne dabei nass zu werden! Nicht alle Daten sind schutzbedürftig und nicht jedes Dokument ist geheim. Anforderungen, die ein Unternehmen nur hausintern erfüllen kann, sind unter Umständen weniger wichtig als eine Anwendung am Laufen zu halten, die mehr Anfragen erhält, als sie verarbeiten kann. Eine *Hybrid Cloud* ist eine Kombination aus Public, Private und Community Clouds, die miteinander kommunizieren können. Der Einsatz einer Hybrid Cloud kann bedeuten, dass es nicht erforderlich ist, eine Private Cloud zu betreiben, die leistungsfähig genug ist, um alle Anfragen in Stoßzeiten zu verarbeiten. Eine Anwendung kann dann zusätzlich auf die Public Cloud zugreifen, anstatt zum Stillstand zu kommen, ein Verfahren, das *Cloud-Bursting* genannt wird. Bei einer Hybrid Cloud geht es jedoch nicht nur darum, dass eine Webanwendung den Zugriff auf zwei verschiedene Cloud-Typen ermöglicht, sondern auch darum, deren Dienste zu kombinieren. Sehen wir uns an, wie Jimmy eine Hybrid Cloud zur Erweiterung seines Geschäfts einsetzen könnte.

Wichtig

Die Unterschiede zwischen Public Cloud, Private Cloud, Community Cloud und Hybrid Cloud sollten Sie kennen.

Jimmy betreibt eine landesweite Kette von Sandwich-Läden und plant die Auslieferung der Ware durch Drohnen. Dazu benötigt er in seiner Private Cloud eine Anwendung zum Berechnen der Flugroute und zur Überwachung der Drohnen. Die Anwendung muss mit der in seiner Private Cloud bereits vorhandenen Auftragsverwaltung zusammenarbeiten. Sie muss außerdem auf die Wettervorhersage-App eines Drittherstellers in der Public Cloud zugreifen können, damit die Drohnen nicht losfliegen, wenn ein Schneesturm droht. Darüber hinaus ist der Zugang zu einer Luftverkehrsüberwa-

chungs-App in einer Community Cloud erforderlich, um zu verhindern, dass es zu Überschneidungen mit den Flugrouten anderer Drohnen, Hubschrauber oder Flugzeuge kommt. Die Gesamtheit dieser Dienste und Anwendungen ist die Hybrid Cloud, die es Jimmy erlaubt, seine Ware durch Drohnen auszuliefern. Wie in den anderen Cloud-Typen gibt es auch in der Hybrid-Cloud drei verschiedene Varianten:

- Hybrid IaaS
- Hybrid PaaS
- Hybrid SaaS

22.3.3 Vorteile der Cloud

Heutzutage werden alle möglichen Aufgaben per Cloud-Computing erledigt. Betrachten wir also kurz die Gründe dafür, statt der herkömmlichen einzelnen Server die Cloud zu nutzen.

Virtualisierung

Die Cloud beruht auf Virtualisierung. Alle in diesem Kapitel beschriebenen Pluspunkte der Virtualisierung treffen auch auf die Cloud zu. Ohne die durch Virtualisierung erzielbaren Einsparungen von Energie und Ressourcen sowie der Sicherheit und einfachen Wiederherstellbarkeit, die eine Virtualisierung bietet, gäbe es keine Cloud.

Gemeinsam genutzte Ressourcen

Echte Hardware kann virtualisiert werden, also teilweise oder vollständig einer VM bereitgestellt werden. Hardware kann kombiniert und dann gemeinsam genutzt werden. Diese gemeinsam genutzten Ressourcen können aus interner oder externer Quelle stammen und einen einzelnen oder mehrere Computer betreffen. Virtualisierung bietet Flexibilität.

Rapid Elasticity

Nehmen wir an, Sie haben eine Webanwendung entwickelt. Wenn Sie das Angebot eines IaaS-Anbieters wie Amazon nutzen, können Sie fürs Erste einen einzigen Server einsetzen, um Ihre Anwendung bereitzustellen. Nun erfreut sich Ihre Anwendung aber wirklich richtig großer Beliebtheit und der eine Server ist völlig überlastet. Keine Sorge! Sie können die Anzahl der Server problemlos erhöhen und diese sogar geografisch verteilen – mit nur wenigen Mausklicks. Das versteht man unter dem Begriff *Rapid Elasticity*.

Ganz nach Bedarf

Und wenn die Nachfrage nach Ihrer Anwendung heftigen Schwankungen unterliegt? Der örtliche Fußballverein möchte die Eintrittskarten zu seinen Spielen online verkaufen. Wenn nicht gerade ein Spiel bevorsteht, ist der Server überhaupt nicht ausgelastet. Vor einem angekündigten Spiel jedoch wird er mit Kartenbestellungen überhäuft. Dank des Cloud-Computings können Sie die Kapazität des Servers ganz nach Bedarf erhöhen oder verringern. Die Leistungsfähigkeit der Anwendung wird entsprechend der aktuellen Nachfrage angepasst.

Ressourcenbündelung

Die Konsolidierung der Hardware bedeutet eine Ressourcenbündelung (engl. *Resource Pooling*). In unserem Beispiel hat ein leistungsstarker Server die Aufgaben von drei anderen Servern übernommen. Stellen Sie sich nun vor, was einem Unternehmen wie Amazon möglich ist. Die AWS-Serverfarmen sind riesige Ressourcenbündelungen, für die ansonsten Millionen auf der ganzen Welt verstreute einzelne Server nötig wären!

Kostenpflichtige Dienste entsprechend der Nutzung

Der einzige Nachteil bei der Nutzung der Public Cloud ist, dass es sich um kostenpflichtige Dienste handelt. Und eins kann ich Ihnen sagen: Die Cloud-Anbieter sind wirklich außerordentlich einfallsreich, wenn es darum geht, für irgendetwas Gebühren zu erheben. In einigen Fällen richten sich die Gebühren nach dem anfallenden Datenverkehr, in anderen nach der Zeitdauer, in der die virtuellen Maschinen in Betrieb sind. Es spielt keine Rolle, wie die Gebühren genau berechnet werden, aber die Kosten orientieren sich an der Nutzung und werden nicht, wie früher üblich, durch einen festen monatlichen oder jährlichen Betrag beglichen.

Cloud-basierte Anwendungen

Bei den Erläuterungen zu SaaS gab es schon den Hinweis auf einen der wichtigsten Gründe, Cloud-Computing zu nutzen: Sämtliche benötigte Software steht zur Verfügung, ohne dass man sie installieren oder aktualisieren muss. Für viele Unternehmen bildet das Office-Paket von Microsoft die Grundlage ihrer Organisation. Die Anwendungen umfassen Word, Excel, PowerPoint und Access – die typischen Büroanwendungen. Microsoft hat das Paket allmählich durch weitere Anwendungen ergänzt, auf die manche Unternehmen (nicht alle) angewiesen sind, beispielsweise Outlook (E-Mail und Kalender), Planner (Projektmanagement), OneNote (zum firmenweiten Teilen von Notizen) und viele andere. Wie kann man als Verwalter der Unternehmenssoftware entscheiden, welche Apps für einen bestimmten Benutzer installiert werden sollen? Wenn es sich um 50 oder 100 Mitarbeiter handelt, macht die Planung, Verteilung und Aktualisierung eine Menge Arbeit.

Mit Office 365 hat Microsoft diese Vorgehensweise in vielerlei Hinsicht verändert. Erstens handelt es sich um einen Dienst, der als kostenpflichtiges Abonnement angeboten wird. Zweitens können die Benutzer nur die Anwendungen installieren, die sie benötigen. Drittens aktualisiert Microsoft die Programme bei Bedarf. Diese Aktualisierungen erfolgen auf allen Computern, die mit dem Internet verbunden sind. Manuelle Aktualisierungen sind nicht erforderlich. Viertens stellt Microsoft Cloud-basierte Versionen der Office-Anwendungen bereit, sodass Benutzer darauf zugreifen können, ohne lokale Installationen vornehmen zu müssen. Durch diese virtuelle Bereitstellung der Anwendungen können Smartphones, Tablets, Laptops und Desktops darauf zugreifen.

Microsoft hat auch Outlook in der Cloud verfügbar gemacht, wodurch das Programm vielleicht zur stabilsten externen E-Mail-Anwendung geworden ist. Der vollständige Kalender und alle empfangenen und gesendeten E-Mails sind von jedem mit dem Internet verbundenen Gerät aus zugänglich. Es handelt sich also nicht um eine abgespeckte Web-basierte Variante, sondern um ein vollwertiges Outlook.

Cloud-basierte virtuelle Desktops

Wir sind in diesem Kapitel bereits die Schritte durchgegangen, die erforderlich sind, um einen virtuellen Desktop in einer VM auf dem lokalen Rechner einzurichten. Eine solche VM kann auch in der Cloud betrieben und über das Internet genutzt werden. Es gibt eine Reihe von Diensten, die es zu einem Kinderspiel machen, Cloud-basierte virtuelle Desktops einzurichten, für deren Nutzung Sie eine monatliche (oder auch stündliche) Gebühr entrichten müssen. Die Bedienung ist manchmal etwas hakelig, aber man kann damit ein paar schöne Tricks anstellen.

Haben Sie sich schon mal die Rechenleistung eines bestens ausgestatteten Desktops und den Komfort eines Laptops gewünscht? Jeder mit dem Internet verbundene Laptop kann einen virtuellen Desktop starten, der über ein Mehrfaches an Rechenleistung verfügt. Zu langweilig? Und wenn Sie Ihren schwachbrüstigen Laptop verwenden könnten, um das neueste Computerspiel zu zocken (mit maximalen Einstellungen!), indem Sie auf einen Spieleserver zugreifen, der bis auf die LEDs so ziemlich alles mitbringt?

Cloud-basierte Speicherdienste

Cloud-basierte Speicherdienste, wie Dropbox oder Box, wurden schnell zu einem durchschlagenden Erfolg und brachten viele Leute dazu, für einen Teil ihres Speicherbedarfs die Cloud zu verwenden.

Dazu gehört immer auch eine App zur Synchronisierung mit dem Desktop, sodass Sie problemlos dafür sorgen können, dass sich an allen Orten (Desktop, Laptop und online) die aktuellen Versionen Ihrer Dateien befinden.

Zusammen mit Office 365 stellt Microsoft Cloud-basierten Speicherplatz zur Verfügung, der auch über SharePoint zugänglich ist.

22.4 Wiederholung

22.4.1 Fragen

1. Die Aufrüstung welcher Komponente einer Wirtsmaschine würde es am wahrscheinlichsten machen, dass Sie mehr virtuelle Maschinen gleichzeitig betreiben können?

   A. CPU

   B. Festplatte

   C. RAM

   D. Windows

2. Was ist der Unterschied zwischen einer VM und einem Emulator?

   A. Eine VM übersetzt die Kommandos einer völlig anderen Plattform mit anderem Prozessor, wodurch sie auf dem Wirtssystem ausgeführt werden können, während ein Emulator eine Umgebung nach Art des Wirtssystems einrichtet und keine Übersetzung durchführt.

   B. Ein Emulator übersetzt die Kommandos einer völlig anderen Plattform mit anderem Prozessor, wodurch sie auf dem Wirtssystem ausgeführt werden können, während eine VM eine Umgebung nach Art des Wirtssystems einrichtet und keine Übersetzung durchführt.

   C. Ein Emulator benötigt ein Wirtssystem, während eine VM direkt auf der Hardware läuft und kein Betriebssystem benötigt.

   D. Eine VM benötigt ein Wirtssystem, während ein Emulator direkt auf der Hardware läuft und kein Betriebssystem benötigt.

3. Welche Funktion gestattet es, den Zustand einer VM abzuspeichern und ihn bei Bedarf wiederherzustellen? (Wählen Sie zwei Antworten aus.)

   A. Sicherungspunkt

   B. Save

   C. Snapshot

   D. Zip

4. Was ist erforderlich, um eine legale Kopie von Windows 10 auf einer virtuellen Maschine in VirtualBox zu installieren?

   A. Eine gültige Lizenz für Windows 10

   B. Original der Windows-10-Installationsmedien

   C. Ein gültiger ESXi-Code

   D. Eine zweite Netzwerkkarte

5. Welchen Vorteil besitzt eine virtuelle Maschine gegenüber einer physischen?

   A. Höhere Geschwindigkeit

   B. Konsolidierung der Hardware

   C. Kein Backup erforderlich

   D. Das Betriebssystem ist Teil der VM

6. Alexandra möchte einen Dienst anbieten, um echte Fotos vom Yeti mit anderen zu teilen, besitzt aber keinen eigenen Server. Wie kann sie auf die Schnelle einen Server für ihren Dienst erstellen?
   A. Public Cloud
   B. Private Cloud
   C. Community Cloud
   D. Hybrid Cloud
7. Der Server mit Yeti-Fotos ist ausgefallen, denn er wurde von Hackern lahmgelegt, weil Alexandra es versäumt hat, Sicherheitsupdates einzuspielen. Sie hat aber schon eine neue Idee und möchte einen Dienst mit Berichten über Sichtungen des Monsters von Loch Ness anbieten. Welchen Dienst könnte sie nutzen, um nicht selbst den Systemadministrator spielen zu müssen?
   A. Software as a Service
   B. Infrastructure as a Service
   C. Platform as a Service
   D. Network as a Service
8. Wie werden leistungsfähige Hypervisoren wie ESXi oft gestartet?
   A. Von Diskette
   B. Von einem USB-Speicherstick
   C. Über die Firmware
   D. Von Windows aus
9. Wie wird eine VM gespeichert, wenn sie nicht läuft?
   A. Per Firmware
   B. Auf einer RAM-Disk
   C. Auf optischen Medien
   D. Als Datei
10. Das Unternehmen YetiFan nutzt einen hausinternen Dienst, um die automatisierten Yeti-Überwachungsstationen zu verwalten. Eine plötzliche große Yeti-Wanderung sorgt dafür, dass die Menge der übermittelten Audio- und Videodaten rasant steigt. Um kurzfristig die Kapazität zu erhöhen, werden virtuelle Server in der Public Cloud erstellt. Welches Modell des Cloud-Computings beschreibt diese Situation?
    A. Public Cloud
    B. Private Cloud
    C. Community Cloud
    D. Hybrid Cloud

22.4.2 Antworten

1. **C.** Das Hinzufügen von RAM ermöglicht es, mehr virtuelle Maschinen gleichzeitig betreiben zu können. Auch die Aufrüstung der Festplatte könnte hilfreich sein, ist hier aber nicht die beste Antwort.
2. **B.** Ein Emulator übersetzt die Kommandos anderer Plattformen, eine VM hingegen spiegelt das Wirtssystem wider.
3. **A, C.** Der gespeicherte Zustand einer VM heißt Snapshot oder Sicherungspunkt und darf nicht mit einem vollständigen Backup verwechselt werden.
4. **A.** Sie benötigen eine gültige Lizenz für Windows 10.
5. **B.** Die Konsolidierung der Hardware ist ein großer Vorteil der Virtualisierung.

6. **A.** Alexandra kann die Public Cloud nutzen, um ihren Dienst anzubieten.
7. **C.** Wenn sie zu einem PaaS-Anbieter wechselt, kann Alexandra sich voll und ganz auf ihren Dienst konzentrieren und die Systemadministration dem Anbieter überlassen.
8. **B.** Ein guter Hypervisor muss nicht besonders groß sein und wird oft von einem USB-Speicherstick gebootet.
9. **D.** VMs sind nichts weiter als Dateien und werden für gewöhnlich auf der Festplatte gespeichert.
10. **D.** Wenn YetiFan die interne Private Cloud mit der Public Cloud verknüpft, handelt es sich um eine Hybrid Cloud.

Tragbare Computer 23

Themen in diesem Kapitel:

- Beschreibung der verschiedenen tragbaren Computer, die es heute gibt
- Erweiterung von tragbaren Computern
- Verwaltung und Wartung von tragbaren Computern
- Aufrüstung und Reparatur von tragbaren Computern
- Fehlerbehebung bei tragbaren Computern

Es gibt Zeiten, in denen man einen Tapetenwechsel braucht und am liebsten mal allein sein möchte, um den großen Ideendurchbruch zu fördern – und manchmal will man einfach nur ein paar Stunden seine Ruhe haben, weil die Kollegen einem auf die Nerven gehen! Bei vielen Tätigkeiten ist dies nur schwer möglich: Sie brauchen den Zugriff auf Ihre Dokumente und Tabellen und können ohne E-Mail und Internet nicht arbeiten. Kurz: Sie benötigen einen Computer, um Ihre Arbeit erledigen zu können!

Tragbare Computer kombinieren Mobilität und Erreichbarkeit und bieten Ihnen so das Beste aus beiden Welten. Mit tragbaren Geräten können Sie den größten Teil (wenn nicht sogar alle) der Aufgaben des Computers auch unterwegs erledigen. Da viele tragbare Computer mit sämtlichen erforderlichen Funktionen ausgestattet sind, können Sie die Arbeit problemlos vom Schreibtisch mit zum Caféhaustisch nehmen.

In diesem Kapitel geht es um die klassischen tragbaren Computer, die im Wesentlichen einen Desktop-PC im Kleinformat darstellen und auf denen Sie Windows, macOS oder eines der vielen Linux-Derivate wie Chrome OS betreiben können.

Hinweis

Auf anderen mobilen Geräten, wie Smartphones und Tablet-Computern, laufen Betriebssysteme wie z.B. Apples iOS für iPad und iPhone, die für kleine Formfaktoren und die Verwendung von Touchscreens optimiert sind. In der Praxis (und in den CompTIA A+-Prüfungen) unterscheiden sich die klassischen tragbaren Computer deutlich von den neuartigen mobilen Geräten wie Smartphones und Tablets. Ihnen ist ein eigenes Kapitel (Kapitel 24, *Mobile Geräte*) gewidmet. In den letzten Jahren hat es im Mobilbereich allerdings eine Vielzahl von Innovationen gegeben und es gibt inzwischen Geräte, bei denen eine scharfe Grenze zwischen herkömmlichen tragbaren Geräten und Smartphones/Tablets kaum noch erkennbar ist.

Geschichte und Konzepte

23.1 Tragbare Geräte

Alle tragbaren Geräte besitzen gewisse gemeinsame Leistungsmerkmale. Die Ausgabe erfolgt über LCD-Bildschirme, bei denen es sich um mächtige 20-Zöller, aber auch um zierliche 10-Zoll-Bildschirme handeln kann. Die Soundqualität reicht von fader Mono-Wiedergabe bis hin zu Pseudo-Surround-Sound. Alle Geräte werden über Akkus mit Gleichstrom betrieben, wenn sie nicht am Stromnetz angeschlossen sind.

Wenn man sich mit jemandem über tragbare Geräte unterhält, denken die meisten an klassische Notebooks, mit eingebautem LCD-Bildschirm, integrierter Tastatur und einem Eingabegerät wie ein Touchpad (Abbildung 23.1). Statt Notebook wird auch der Begriff Laptop verwendet. Ein Laptop arbeitet als eigenständiger PC, aber wegen der Mobilität müssen immer Kompromisse eingegangen werden: Preis,

Gewicht, Größe, Akkulaufzeit, Rechenleistung, Eingabegeräte, Anschlüsse, Laufwerke, Unterstützung von Hardware-Aufrüstungen, Speicherkapazität, Lebensdauer und der Umfang der Garantie. Einen geeigneten tragbaren Computer zu finden, ist einfacher, wenn Sie wissen, wofür er benutzt werden soll, damit Sie Ihre Suche auf Geräte beschränken können, die über die erforderlichen Merkmale verfügen, und Geräte ausschließen können, die einen inakzeptablen Kompromiss darstellen.



Abb. 23.1: Ein älteres Notebook

23.1.1 Klassifikation

Das ungezügelte Herumexperimentieren und die Innovationen im Mobilbereich haben zu neuen Gerätekategorien geführt und andere abgelöst. Neue Gerätekategorien und die dazugehörigen Marketingbegriffe überschwemmen den Markt in einem Jahr und die Grenzen zwischen den verschiedenen Kategorien verschwimmen zunehmend. Und in wenigen Jahren sind sie schon wieder vom Markt verschwunden.

Die CompTIA A+-Lernzeile konzentrieren sich zwar nicht auf diese Begriffe und Kategorien, dennoch sollte man sie kennen. Die Fähigkeit, mobile Geräte zu kategorisieren, erleichtert es, für eine bestimmte Aufgabe gedachte Geräte auszuwählen. Sie ist auch hilfreich dabei, die beste Art der Fehlerbehebung zu ermitteln. Da die Grenzen zwischen den Gerätekategorien fließend sind, schließen sie sich nicht notwendigerweise gegenseitig aus. Nicht selten trifft mehr als eine Bezeichnung auf ein einziges Gerät zu.

Manche Begriffe beziehen sich auf die Größe oder den Zweck klassischer Notebooks/Laptops, man muss nur wissen, dass heutige Notebooks (getrieben durch den Erfolg des MacBook Air) beträchtlich dünner, leichter und leistungsstärker sind als zu den Zeiten, als diese Begriffe geprägt wurden (Abbildung 23.2).



Abb. 23.2: Ein voluminöser älterer Laptop (links) und das besonders schlanke MacBook Air (rechts)

- Ein tragbarer Computer, der als *Desktop-Ersatz* dienen soll, benötigt einen großen Bildschirm, eine komplette Tastatur, eine eigenständige Grafikkarte, einen aktuellen Notebookprozessor, eine Menge Festplattenspeicherkapazität und Arbeitsspeicher, haufenweise Anschlüsse und vielleicht ein optisches Laufwerk (wie der tragbare Computer links in Abbildung 23.3). Hier zählt die Leistung mehr als die Portabilität, da das Gerät alles kann, was die meisten Benutzer mit einem Desktop-PC machen würden, und weil es keine Kompromisse bei der Leistung eingeht, nur um ihn ein paar Kilo leichter zu machen oder dafür zu sorgen, dass die Akkus eine Stunde länger durchhalten.



Abb. 23.3: Desktop-Ersatz (links) neben einem normalen Laptop (rechts)

- *Spiele-Laptops*, die oft ein auffälliges Design besitzen, bringen typischerweise den neuesten und schnellsten Prozessor, eine Grafikkarte der Spitzenklasse, massenhaft RAM, eine große SSD sowie ein hochwertiges Display mit. Oft gibt es auch wohlüberlegte Extras, wie z.B. hochgradig konfigurierbare Tastaturen.
- Das *Chromebook* ist ein tragbarer Computer, auf dem Googles Linux-basiertes Chrome OS läuft. Chromebooks konzentrieren sich auf Webanwendungen und setzen auf die Nutzung des praktisch unbegrenzten Speicherplatzes in der Cloud und Anwendungen, die als *SaaS* (*Software as a Service*) über das Web bereitgestellt werden. Weil sie den Großteil der Arbeitslast nicht selbst erledigen, haben Chromebooks den Ruf, billig und schlicht zu sein, aber Premium-Chromebooks sind zunehmend gebräuchlich.

Die Kategorisierung von Geräten, deren Größe derjenigen klassischer Notebooks nahekommt, ist ebenfalls wichtig, weil sie die Grenze zwischen mobilen Geräten und tragbaren Computern verschwimmen lassen.

- Die heutzutage unter der Bezeichnung *2-in-1* vermarkteten Geräte sind im Grunde genommen Touchscreencomputer, die irgendwo zwischen Tablet und Laptop einzuordnen sind. In Kapitel 24 werden wir uns eingehender mit ihnen befassen.
- Die Bezeichnung *Convertible* wird für einen Laptop benutzt, der irgendeinen Mechanismus besitzt, damit man ihn wie ein Tablet verwenden kann. So gibt es beispielsweise Convertibles, bei denen der Bildschirm komplett abnehmbar ist und als eigenständiges Tablet nutzbar ist. Bei anderen Geräten gibt es verschiedene Formen spezieller Scharniere.
- Ein Laptop-Tablet-*Hybride* ist meist ein Gerät mit dem Formfaktor eines Tablets, das dafür ausgelegt ist, eine ansteckbare Tastatur aufzunehmen. Die Tastatur gehört in manchen Fällen zum Lieferumfang und dient oft gleichzeitig als Abdeckung bzw. Schutz für das Tablet (Abbildung 23.4). Bei anderen Geräten ist eine normale, wenn auch oft sehr kleine Tastatur verbaut. Mitunter wird für Geräte, die für die Bedienung mit einem Stift (»Stylus«) ausgelegt sind, auch die Bezeichnung *Slate* gebraucht.



Abb. 23.4: Microsoft Surface Pro 6 mit Tastatur/Abdeckung (Foto mit freundlicher Genehmigung von Microsoft)

Hinweis

Geräte, die zu einer der neuartigen Kategorien wie Convertible oder Hybrid gehören, sind oft dafür ausgelegt, in der Hand gehalten, gedreht oder herumgereicht zu werden. Windows unterstützt daher nun ebenfalls die automatische Bildschirmausrichtung anhand der Orientierung des Geräts, wie Sie es seit Jahren von Smartphones und Tablets kennen. Wenn Sie solch ein Gerät längere Zeit genutzt haben, wissen Sie auch, dass es gelegentlich zu Schwierigkeiten mit dem Lagesensor kommt, der für die Bildschirmausrichtung zuständig ist. Wie man solche Probleme löst, erfahren Sie im Abschnitt 23.5, *Fehlerbehebung bei tragbaren Computern.*

1001

23.1.2 Eingabegeräte

Es gibt eine ganze Reihe verschiedener Eingabegeräte für tragbare Computer. Die meisten besitzen eine vollständige Tastatur und ein Zeigegerät zur Steuerung des Mauszeigers.

Tastaturen

Laptop-Tastaturen unterscheiden sich etwas von normalen Desktop-PC-Tastaturen, weil einfach nicht so viel Platz zur Verfügung steht. Es handelt sich zwar um QWERTZ-Tastaturen, aber die verschiedenen Hersteller gehen bei der Tastengröße und den Positionen der Tasten für Sonderzeichen gewisse Kompromisse ein. Fast alle Notebook-Tastaturen verwenden eine Funktionstaste [FN], um bestimmten Tasten eine dritte Belegung zuzuweisen. Entweder hält man die Taste [FN] gedrückt, um auf die zusätzliche Funktion zuzugreifen, oder aber man muss sie gedrückt halten, um auf die normalen Funktionstasten [F1] bis [F12] zuzugreifen (Letzteres ist häufiger).

Abbildung 23.5 zeigt eine normale Desktop-Tastatur im Vergleich zu einer großen Notebook-Tastatur. Wie Sie sehen, besitzt Letztere keinen separaten Zehnerblock. Um diesen zu verwenden, betätigen Sie die Taste [FN] (hier unten links), um für die gekennzeichneten Buchstabentasten die Belegung mit Ziffern einzustellen.



Abb. 23.5: Tastaturen im Vergleich

Hinweis

Mit der Taste [FN] lassen sich oft weitere Funktionen aufrufen, wie z.B. das Umschalten der Anzeige auf einen externen Bildschirm oder das Abschalten der Tastaturbeleuchtung, um Energie zu sparen.

Zeigegeräte

Auch bei Notebooks müssen Sie auf irgendeine Weise den Mauszeiger steuern, aber aufgrund der geringen Geräteabmessungen mussten sich die Hersteller etwas einfallen lassen. Laptops besitzen für gewöhnlich USB-Anschlüsse, an die Sie dieselben Zeigegeräte wie auch am Desktop anschließen können. Bei älteren Notebooks war auch die Verwendung von Trackballs üblich, die wie eine Maus angeschlossen und am seitlichen oder vorderen Rand des Geräts befestigt wurden.

IBM entwickelte dann den *TrackPoint*, eine Art Joystick in der Größe eines Bleistiftradiergummis, der sich inmitten der Tastatur befindet (Abbildung 23.6). Mit dem TrackPoint können Sie den Mauszeiger über den Bildschirm bewegen, ohne die Hände von der Tastatur nehmen zu müssen. Sie benutzen dabei Ihren Zeigefinger zur Steuerung des Mauszeigers und zwei Knöpfe unterhalb der Leertaste, um mit der linken bzw. rechten Maustaste zu klicken. IBM hat dieses Zeigegerät an andere Hersteller lizenziert und man findet es auch bei aktuellen Laptops.



Abb. 23.6: IBMs TrackPoint

Am häufigsten sieht man jedoch *Touchpads* (Abbildung 23.7), eine flache, berührungsempfindliche Fläche direkt vor der Tastatur. Bei der Bedienung des Touchpads bewegen Sie einfach einen Finger über die Oberfläche, um den Mauszeiger zu bewegen. Ein einfaches bzw. doppeltes Antippen der Oberfläche entspricht einem Klick oder Doppelklick. Alternativ können Sie auch die unterhalb des Touch-

pads befindlichen Tasten zum Klicken verwenden. Die meisten Leute haben bei der Bedienung des Touchpads nach wenigen Minuten den Bogen raus. Der größte Vorteil des Touchpads gegenüber den älteren Zeigegeräten ist das Fehlen beweglicher Teile, was die Lebensdauer stark beanspruchter Notebooks deutlich erhöhen kann.



Abb. 23.7: Das Touchpad eines Laptops

Einige Hersteller setzen auch eine als *Multitouch* bezeichnete Technologie ein, bei der Sie mittels verschiedener Fingergesten bestimmte Aktionen auslösen können, wie beispielsweise Hinein- oder Herauszoomen, bildschirmweises Blättern usw. Das Multitouch-Trackpad von Apples Laptops spielte hier eine Vorreiterrolle, und die damit einhergehenden Verbesserungen sorgten dafür, dass das Fehlen einer Maus bei vielen Laptops nicht mehr als hinderlich empfunden wird.

Wichtig

Es kommt gelegentlich vor, dass man beim Tippen das Touchpad unabsichtlich mit der Handfläche »bedient«. Um das zu verhindern, gibt es bei manchen Geräten einen Schalter oder eine Tastenkombination zum Abschalten des Touchpads. Neuere Touchpad sind für gewöhnlich in der Lage, solche unbeabsichtigten Berührungen automatisch zu erkennen und reagieren darauf nicht.

Dem Trend folgend, dass Smartphones und Tablets die herkömmlichen tragbaren Computer beeinflussen, sind immer mehr Laptops mit einem Touchscreen ausgestattet, die es gestatten, komplexe Aktionen durch verschiedene Gesten auszuführen. Das trifft auch für ansonsten ganz normale Laptops zu, manche Geräte sind hingegen dafür gedacht, sowohl als Tablet als auch als Laptop benutzt zu werden. In Kapitel 24 werden wir uns eingehender mit Touchscreens befassen.

Wichtig

Verwenden Sie das Dialogfeld EINSTELLUNGEN|GERÄTE|MAUS oder das Applet MAUS in der Systemsteuerung, um das Touchpad zu konfigurieren. Hier können Sie die SCROLLGESCHWINDIGKEIT und einiges mehr einstellen.

Webcams und Mikrofone

Die Möglichkeit, mit tragbaren und mobilen Geräten in Echtzeit über Video miteinander zu kommunizieren, ist heutzutage gang und gäbe. Daher sind viele Geräte, Laptops inklusive, mit (mindestens) einem Mikrofon und einer auf den Benutzer ausgerichteten Kamera ausgestattet – einer Webcam,

wenn es sich um einen Laptop handelt. Ein einzelnes Mikrofon reicht zwar aus, um die Stimme des Benutzers aufzunehmen, mit weiteren Mikrofonen kann jedoch eine Unterdrückung von Umgebungsgeräuschen stattfinden, wodurch die Tonqualität verbessert wird.

Die meisten Leute verwenden das Mikrofon vielleicht nur zusammen mit der Webcam, aber eine zunehmende Zahl an Programmen unterstützt Sprachbefehle. Beispielsweise bewirbt Microsoft die Cortana-Funktionalität von Windows 10. Jeder Benutzer, dessen System über ein Mikrofon verfügt, kann per Sprachbefehl suchen und andere Aktionen ausführen – sofern er denn damit einverstanden ist, dass Windows alles mithören kann, was in Mikrofonreichweite gesagt wird.

Der Nachteil dieser zunehmend allgegenwärtigen Eingabegeräte ist das Sicherheitsrisiko, das sie darstellen. Es ist ja schon schlimm genug, wenn ein bösartiger Hacker oder der Nachrichtendienst irgendeines Staates es schafft, Malware auf meinem Rechner zu installieren und alles mitbekommt, was ich anklicke oder schreibe, aber die Risiken vervielfachen sich, wenn sie auch noch alles hören und sehen können, was in der Umgebung meines Computers geschieht. Viele Webcams verfügen deswegen über eine LED, die anzeigt, dass eine Aufnahme läuft, für eingebaute Mikrofone gibt es jedoch keine Betriebsanzeige. In manchen Fällen kann die Aufnahmeanzeige dank Sicherheitsschwachstellen sogar deaktiviert werden.

23.1.3 Bildschirme

Laptops gibt es in den verschiedensten Größen und Preisklassen. Ein wichtiger Faktor für die Gesamtkosten eines Laptops ist die Größe des LCD-Bildschirms. Die Bildschirme der meisten Laptops besitzen Diagonalen zwischen 10,1 und 17,3 Zoll, es gibt aber auch Geräte mit größeren Bildschirmen.

Wichtig

Laptop-LCDs besitzen ebenso wie TFT-Bildschirme einen Inverter (bei Verwendung einer Kaltkathodenlampe) und eine Hintergrundbeleuchtung (Kaltkathodenlampe oder LED). Das ist Ihnen aus Kapitel 17 bereits bekannt. Sie dürfen Prüfungsfragen zu Laptop-Bildschirmen erwarten, sollten aber wissen, dass sich diese kaum von normalen LCD-Bildschirmen unterscheiden. Ein wesentlicher Unterschied ist, dass es eine Antenne und gegebenenfalls eine Kamera und ein Mikrofon gibt, aber dazu später mehr.

Früher waren Bildschirme mit einem Seitenverhältnis von 4:3 üblich, aber heutzutage findet man sie höchstens noch bei speziellen Laptops, die besonders rauen Umgebungen standhalten müssen. Fast alle »normalen« Laptops verwenden jetzt eins von zwei gängigen Widescreen-Formaten. Beim *Seitenverhältnis* handelt es sich um das Verhältnis von Bildschirmbreite zu Bildschirmhöhe, wie Sie aus Kapitel 19 wissen. Es gibt verschiedene andere Seitenverhältnisse, aber die meisten weisen das Format 16:9 oder 16:10 auf. Sehr alte Laptops hatten ein Bildseitenverhältnis von 4:3.

Die Oberfläche von Laptop-LCDs kann *matt* oder *spiegelnd* sein. Die matten Oberflächen waren jahrelang der Industriestandard und boten einen guten Kompromiss zwischen Farbumfang und Entspiegelung. Die besseren Bildschirme haben einen breiteren Sichtwinkel und eine bessere Reaktionszeit. Der größte Nachteil bei den matten Laptop-Bildschirmen ist, dass die Farben in heller Umgebung recht blass wirken. Einen solchen Laptop irgendwo in einem Biergarten zu verwenden, ist bei normalem Tageslicht fast hoffnungslos.

2006 haben die Hersteller Laptops mit Hochglanzbildschirmen eingeführt, die schnell in allen Regalen zu finden waren. Die spiegelnde Oberfläche sorgt für einen höheren Kontrast, sattere Farben und einen breiteren Sichtwinkel als die matten Bildschirme. Der Nachteil bei den Hochglanzbildschirmen ist, dass sie im Gegensatz zu den Behauptungen der Hersteller nahe gelegene Gegenstände und damit auch den vor dem Bildschirm sitzenden Benutzer recht stark reflektieren! Durch die satteren Farben und den höheren Kontrast lässt sich zwar tagsüber draußen mit den Geräten besser arbeiten, aber dafür müssen Sie erhöhte Reflexionen in Kauf nehmen.

Seit LED-Hintergrundbeleuchtungen verfügbar sind, haben sich viele Hersteller wieder entspiegelten Bildschirmen zugewendet, die allerdings den früher gebräuchlichen matten Bildschirmen nicht ganz

das Wasser reichen können. Wenn die LED-Helligkeit hoch eingestellt ist, sind das aber sehr schöne Bildschirme. (Bildschirme mit LED-Hintergrundbeleuchtung kommen im Abschnitt 23.5, *Fehlerbehebung bei tragbaren Computern*, erneut zur Sprache.)

Die meisten LCD/LED-Bildschirme verwenden die TN-Technologie, die Sie aus Kapitel 17 kennen. Bei einigen Modellen finden *IPS-Panel* (*In-Plane-Switching*) Einsatz, um einen höheren Sichtwinkel und sattere Farben zu erzielen. IPS-Bildschirme findet man vor allem bei teuren, professionellen Geräten, die als Desktop-Ersatz dienen.

Zwei Anzeigetechnologien werden Sie bei tragbaren Computern *nicht* finden: Plasma-Bildschirme und *OLED* (*Organic Light-Emitting Diode*). Plasma-Bildschirme benötigen sehr viel mehr Energie als LCD-Bildschirme und sind daher für tragbare Computer völlig ungeeignet. OLEDs sind im Vergleich zu LCDs beim Energieverbrauch sparsam, aber noch immer so teuer, dass sie derzeit nur bei Smartphones und Tablets eingesetzt werden. In Kapitel 24 werden OLEDs eingehender vorgestellt.

Wichtig

In den CompTIA A+-Lernzielen ist von OLED-Bildschirmen für Laptops die Rede. Einige Hersteller haben in jüngster Zeit mit OLED-Bildschirmen experimentiert, aber die meisten halten sich bis auf Weiteres von der Technologie fern. Notebooks mit OLED-Bildschirm werden Ihnen in der Praxis kaum begegnen, für die Prüfung sollten Sie jedoch wissen, dass es sie gibt!

23.2 Erweiterung und Aufrüstung von tragbaren Computern

In der Steinzeit tragbarer Computer mussten Sie einen Haufen Geld für nicht einmal erweiterungsfähige Geräte hinlegen, die sich bereits nach einiger Zeit kaum mehr sinnvoll nutzen ließen. Einen Laptop aufrüsten? Externe Geräte anschließen? Falls überhaupt, gab es nur wenige Alternativen. Man musste viel Geld für Geräte bezahlen, die bereits nach einem Jahr mit der technischen Entwicklung kaum mehr mithalten konnten und nach zwei Jahren funktional veraltet waren.

Moderne tragbare Computer bieten viele Möglichkeiten zur Erweiterung ihrer Funktionen. Über externe Erweiterungsbusse können Sie die meisten tragbaren Computer mit völlig neuen Funktionen ausstatten und z.B. Scanner oder mobile Drucker anschließen. Die aktuellen drahtlosen Technologien nutzen Sie einfach durch Einsetzen einer Karte in den entsprechenden Steckplatz Ihres Laptops.

Ich werde zunächst monofunktionale Anschlüsse beschreiben und mich dann den Netzwerkoptionen zuwenden. Danach betrachten wir Kartensteckplätze und behandeln abschließend Anschlüsse, die für verschiedene Zwecke nutzbar sind.

23.2.1 Monofunktionale Anschlüsse

Alle tragbaren Computer besitzen monofunktionale Anschlüsse. Sie werden beispielsweise kaum einen tragbaren Computer finden, der keinen Audioausgang besitzt. Und Laptops besitzen oft einen Videoausgang zum Anschluss eines externen Bildschirms. Allerdings erfreuen sich drahtlose Bildübertragungen und Bildschirmfreigaben als Alternative wachsender Beliebtheit.

Die Anschlüsse von tragbaren Computern funktionieren genauso wie Anschlüsse eines Desktop-PCs. Sie schließen ein Gerät an einem bestimmten Anschluss an, und nach dem Einschalten des Rechners funktioniert das Gerät, sofern das Betriebssystem über die erforderlichen Treiber verfügt.

Audio

Für den Kopfhöreranschluss wird eine 3,5-mm-Standardbuchse für Klinkenstecker verwendet. Einige tragbare Computer besitzen außerdem einen Mikrofonanschluss gleicher Größe (Abbildung 23.8). Wie beim Desktop-PC können Sie am Audioausgang zur Musikwiedergabe Kopfhörer, Lautsprecher oder sogar ein Surround-Sound-System anschließen.



Abb. 23.8: Standard-Audioanschlüsse

Die Ein- und Ausgabe des Tons steuern Sie unter Windows über das entsprechende Applet in der Systemsteuerung, in macOS über die Systemeinstellung TON, oder durch irgendwelche Regler am Laptop. Das Gerät in Abbildung 23.9 besitzt beispielsweise einen Stummschalter oberhalb der Tastatur. Bei den meisten Geräten befinden sich an derselben Stelle auch Tasten zum Erhöhen bzw. Senken der Lautstärke. Andere Geräte verwenden oft eine Kombination aus FN und einer weiteren Taste zum Ein- und Ausschalten der Tonausgabe, zum Wiedergeben und Pausieren oder zum schnellen Vor- und Rücklauf.



Abb. 23.9: Stummschalter eines Laptops

Bildschirm

Zum Anschließen eines externen Monitors verfügen die meisten Laptops über einen digitalen Anschluss wie HDMI, Mini-HDMI, Micro-HDMI, DisplayPort (USB Typ C und Thunderbolt) oder DVI. Bei älteren Rechnern findet sich möglicherweise sogar noch ein analoger VGA-Anschluss. Nach Anschluss eines zweiten Bildschirms können Sie einstellen, ob auf dem externen Bildschirm nur der Laptop-Bildschirm oder ein erweiterter Desktop angezeigt wird, auf den Sie Fenster verschieben können. Das unterstützen zwar nicht alle Geräte, bei den meisten ist es aber der Fall.

Die meisten Notebooks verwenden eine Kombination aus FN und einer zusätzlichen Taste, um die verschiedenen Varianten der Reihe nach darzustellen. Beachten Sie in Abbildung 23.10 die Zusatzfunktionen, die in Kombination mit der Taste FN zugänglich sind, wie etwa bei der Taste F2. Halten Sie FN gedrückt und betätigen Sie F2, um den Anzeigemodus zu wechseln.

Hinweis

Nicht alle Laptops verwenden zum Wechseln des Anzeigemodus solche Tastenkombinationen. Unter Umständen müssen Sie in der Systemsteuerung im Applet ANZEIGE ein Kontrollkästchen markieren. Sie können jedenfalls davon ausgehen, dass es eine Möglichkeit gibt, den Anzeigemodus zu wechseln, sofern der Laptop einen zweiten Bildschirm unterstützt.



Abb. 23.10: Notebooktastatur mit der Funktionstaste FN, die in Kombination mit F2 verschiedene Anzeigemodi aktiviert

Den Anzeigemodus können Sie über die Anzeigeeinstellungen Ihres Betriebssystems festlegen. In Windows 10 finden Sie diese Möglichkeit im Bereich ANZEIGE der Einstellungen-App. Öffnen Sie die App und wählen Sie SYSTEM|ANZEIGE aus. Scrollen Sie nach unten, bis die Option MEHRERE BILDSCHIRME angezeigt wird (Abbildung 23.11), und klicken Sie das Einblendmenü an. DIESE ANZEIGEN ERWEITERN sorgt dafür, dass Ihr Desktop sowohl den Laptop als auch den externen Bildschirm umfasst. Die Auswahl DIESE ANZEIGEN DUPLIZIEREN stellt auf beiden Bildschirmen denselben Inhalt dar. Diesen Modus verwenden Sie beispielsweise bei Präsentationen, nicht zum Arbeiten.

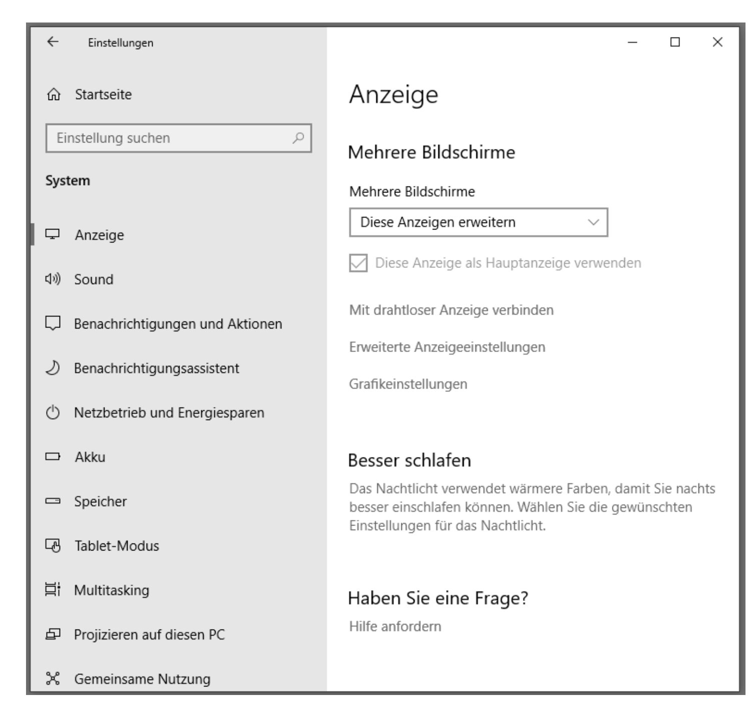


Abb. 23.11: Die Option MEHRERE BILDSCHIRME in Windows 10

Chipkartenleser

Genau genommen handelt es sich nicht um einen Anschluss, aber insbesondere bei Laptops, die Geschäftsleute zur Zielgruppe haben, findet sich an einer der beiden Seiten des Geräts ein sehr schmaler Schlitz von der Breite einer Kreditkarte. Nein, er dient nicht zur Aufnahme einer Steck- oder Speicherkarte, sondern als Chipkartenleser. Wenn Ihnen schon einmal eine Kreditkarte mit einem kleinen metallischen Chip untergekommen ist, dann haben Sie auch schon eine Chipkarte gesehen (Abbildung 23.12). Für Chipkarten gibt es zahllose Anwendungen, hier ist jedoch entscheidend, dass Sie sich mit Ihrer persönlichen Chipkarte und einer PIN an einem Laptop anmelden können, wenn dieser über einen eingebauten oder per USB angeschlossenen Chipkartenleser verfügt. Die Verwendung von Chipkarten zur Authentifizierung von Benutzern werden wir uns in Kapitel 27 näher ansehen.



Abb. 23.12: Chipkarte

23.2.2 Netzwerk

Es gibt heutzutage wohl kaum einen tragbaren Computer, der sich nicht über mindestens eine Schnittstelle mit einem Netzwerk verbinden lässt. Die aktuellen Geräte bringen nicht nur drahtloses Netzwerk nach IEEE 802.11 mit, sondern verfügen auch über Bluetooth oder kabelgebundenes Ethernet. Im Großen und Ganzen funktioniert hier alles so, wie Sie es aus den vorhergehenden Kapiteln bereits kennen, aber hier und da stößt man dann bei tragbaren Computern doch auf gewisse Eigenheiten. (Tablets und Smartphones bieten sogar noch mehr Optionen, wie Sie in Kapitel 24 sehen werden.)

Drahtlos

Bei den heutigen tragbaren Computern ist WLAN fast immer schon Bestandteil des Chipsatzes, sodass einer Internetverbindung über einen WAP nichts im Wege steht. Bei älteren Laptops sind die Standards 802.11g und 802.11n gebräuchlich, während neuere Modelle 802.11ac verwenden.

Hinweis

Aktuelle Geräte werden mit 802.11ac ausgeliefert, allerdings sollten Sie damit rechnen, dass Ihnen in der Praxis auch die älteren Standards begegnen werden, zumal die Geräte inzwischen leistungsfähig genug sind, um immer langlebiger zu werden.

Bluetooth

Die meisten tragbaren Computer nutzen auch Bluetooth, wenngleich es noch nicht so verbreitet ist wie drahtlose Netzwerke nach IEEE 802.11. Bluetooth ist insbesondere bei Laptops wirklich praktisch, da es Ihnen die Verwendung drahtloser Mäuse, Tastaturen und Headsets erlaubt und Sie mit Smartphones, Lautsprechern und anderen Bluetooth-Geräten kommunizieren können.

Hardware-Schalter

Laptops mit eingebautem WLAN, Mobilfunkzugang, GPS oder Bluetooth besitzen irgendeine Art Schalter, mit der sich die Antennen abschalten lassen. Das ermöglicht es Ihnen, das Gerät auch in Bereichen zu verwenden, in denen Strahlungsemissionen untersagt sind (wie z.B. im Flugzeug). Es gibt sowohl mechanische Schalter, wie den in Abbildung 23.13, oder es kommen wieder Tastenkombinationen mit der Taste FN zum Einsatz. Im Übrigen sollten Sie Bluetooth und WLAN abschalten, wenn Sie diese nicht verwenden, um dadurch Energie zu sparen und die Akkulaufzeit zu erhöhen.



Abb. 23.13: Ein mechanischer Schalter

> **Wichtig**
>
> Mittels mechanischer Schalter oder spezieller Tastenkombinationen mit der FN-Taste können Sie Funktionalitäten wie WLAN, Mobilfunk oder Bluetooth ein- und ausschalten. Deaktivieren Sie diese Funktionen in Situationen, in denen eine lange Akkulaufzeit wichtiger ist als der Netzwerkzugang.

Kabelgebundenes Ethernet

Die meisten Laptops normaler Größe besitzen eine RJ-45-Buchse zum Anschluss eines UTP-Ethernet-Kabels (Abbildung 23.14). Sie finden auch hier oft LEDs zur Verbindungsstatus- und Aktivitätsanzeige. Allerdings müssen Sie sich darüber im Klaren sein, dass viele der heutigen Laptops und Hybriden auf kabelgebundenes Ethernet verzichten.



Abb. 23.14: Ethernet-Anschluss eines Laptops

Bei der RJ-45-Buchse eines Laptops sind zwei Punkte zu beachten. Zum einen gibt es, anders als bei Bluetooth und WLAN, keinen Hardware-Schalter, um sie ein- und auszuschalten. Sie können die interne Netzwerkkarte aber, wie alle anderen Netzwerkkarten auch, im Geräte-Manager oder im BIOS deaktivieren. Zum anderen sind die Buchsen relativ empfindlich und leiern bei häufigem Gebrauch

aus. Wenn Sie ein Notebook an ein drahtgebundenes Netzwerk anschließen und das Betriebssystem keine Verbindung anzeigt, dann sollten Sie die RJ-45-Buchse überprüfen.

23.2.3 Erweiterungskarten für tragbare Computer

Die Hersteller von tragbaren Computern haben Methoden entwickelt, um es Ihnen zu ermöglichen, ihr Gerät über spezielle Anschlüsse zu erweitern. Diese Anschlüsse werden allgemein als *Erweiterungssteckplätze* bezeichnet. Vor vielen Jahren hat die *PCMCIA* (*Personal Computer Memory Card International Association*) Standards für tragbare Computer definiert, insbesondere für Erweiterungskarten. Sie waren früher sehr verbreitet, aber angesichts der Dominanz von USB sind sie so gut wie ausgestorben. Der letzte Standard hieß *ExpressCard*.

ExpressCard

Die ExpressCard gibt es in zwei Breiten, 54 mm und 34 mm, die als ExpressCard/34 und ExpressCard/54 bezeichnet werden. Abbildung 23.15 zeigt die beiden ExpressCard-Varianten. Beide Kartenvarianten sind 75 mm lang und 5 mm tief.



Abb. 23.15: 34 und 54 mm breite ExpressCards

Sie können ältere Laptops mit einem ExpressCard-Steckplatz auf verschiedene Weise aufrüsten. Am verbreitetsten sind Chipkartenleser, wodurch der Laptop beispielsweise SD-Karten lesen kann, und Mobilfunkkarten. Letztere ermöglichen es, über eine Mobilfunkverbindung auf das Internet zuzugreifen, wenn man einen entsprechenden Vertrag mit einem Mobilfunkanbieter abgeschlossen hat. Es gibt auch WLAN-Erweiterungskarten, die aber aufgrund der Beschränkungen der ExpressCard-Technologie nur 802.11n unterstützen, nicht aber die neueste Version.

ExpressCards werden entweder über den USB-2.0-Bus oder den PCI-Express-Bus angebunden. Das führt zu enormen Geschwindigkeitsunterschieden. Die vergleichsweise überraschend langsame USB-Variante bietet einen maximalen Durchsatz von 480 Mbps. Die PCIe-Variante bringt es hingegen auf stolze 2,5 Gbps bei unidirektionaler Kommunikation.

In Tabelle 23.1 sind die beiden noch erhältlichen ExpressCard-Varianten und deren Durchsatz aufgeführt.

Standard	Maximaler theoretischer Durchsatz
ExpressCard mit USB-2.0-Bus	480 Mbps
ExpressCard mit PCIe-Bus	2,5 Gbps

Tabelle 23.1: Geschwindigkeiten von ExpressCards

23.2.4 Steckplätze für Speicherkarten

Viele tragbare Computer besitzen Steckplätze für Flash-Speicherkarten, die es gestatten, dem tragbaren Gerät zusätzliche Speicherkapazität hinzuzufügen. Mittels dieser Steckplätze ist auch eine schnelle Datenübertragung von der Speicherkarte auf den tragbaren Computer (und umgekehrt) möglich. Die verfügbaren Varianten wie SD oder Micro-SD sind Ihnen bereits aus Kapitel 10 bekannt.

23.2.5 Mehrzweckanschlüsse

Laptops verfügen nur selten über alle benötigten oder erwünschten Hardwarekomponenten. Aktuelle Laptops bieten für gewöhnlich wenigstens USB-Anschlüsse, über die Sie die Hardwareausstattung erweitern können. Einige spezialisierte Laptops stellen weiterhin die älteren Erweiterungsanschlüsse (PS/2, serielle RS-232-Anschlüsse, eSATA, FireWire usw.) zur Installation von Peripheriegeräten zur Verfügung, während andere Modelle lieber modernere Anschlüsse wie Thunderbolt mitbringen. Und wenn Sie Glück haben, dann ist vielleicht sogar eine Dockingstation erhältlich, damit Sie die Peripheriegeräte nicht immer wieder einzeln anschließen müssen.

USB, Thunderbolt, FireWire und eSATA

USB (*Universal Serial Bus*), Thunderbolt, FireWire (bzw. IEEE 1394) und eSATA erlauben es, dass Benutzer Geräte an ihr System anschließen können, während es läuft. Es muss für den Anschluss von Peripheriegeräten also nicht erst neu gestartet werden. Bei Verwendung von USB und FireWire schließen Sie einfach den Stecker an und können loslegen! Da mobile Rechner intern weniger erweiterungsfähig als Desktop-Rechner sind, werden für den Anschluss von Peripheriegeräten an Laptops vorwiegend USB und Thunderbolt (und in geringerem Maße FireWire) genutzt (siehe Abbildung 23.16).



Abb. 23.16: Per USB an einen Laptop angeschlossene Geräte

Dockingstationen

Eine *Dockingstation* bietet spezifische und multifunktionale Anschlüsse (Abbildung 23.17). Eine klassische Dockingstation besitzt einen herstellerspezifischen Anschluss, aber dank der hohen Geschwindigkeit von USB 3.x und Thunderbolt 2 und 3 sind universelle Dockingstationen gebräuchlicher geworden. Dockingstationen sind für kleinere Laptopmodelle mit wenigen Anschlüssen eine hervorragende Begleitausstattung.



Abb. 23.17: Dockingstation

Portreplikatoren

Ein *Portreplikator* bietet die wichtigste Funktionalität einer Dockingstation, aber in einem kleineren und portableren Format, nämlich die Unterstützung für Anschlüsse, die dem Laptop fehlen. Ein moderner über USB C angeschlossener Portreplikator bietet eine Reihe von Anschlüssen, wie VGA, HDMI, USB Typ A (2, 3, 3.1), RJ-45 und mehr. Portreplikatoren sind bestens dazu geeignet, die Fähigkeiten besonders dünner und leichter Laptops zu erweitern.

USB-Adapter

Wenn nicht schon alle USB-Anschlüsse belegt sind, können Sie einen USB-Adapter verwenden, um alle erdenklichen Geräte anzuschließen. Wenn es um Laufwerke oder Verbindungen geht, die nur gelegentlich benötigt werden, versetzen solche Adapter Sie in die Lage, Ihr Gerät viel freizügiger zu benutzen.

Kabelgebundenes Ethernet und optische Laufwerke sind zwei schöne Beispiele. Ich weiß nicht, wie Sie das sehen, aber ich habe seit Monaten kein optisches Laufwerk mehr benutzt. Und ich bin mir auch nicht sicher, wie lange es her ist, dass ich zuletzt ein Ethernet-Kabel an meinen Laptop angeschlossen habe. Ein USB-RJ45-Adapter und ein optisches Laufwerk mit USB-Anschluss würden es mir jederzeit ermöglichen, kabelgebundenes Ethernet bzw. optische Medien zu nutzen, wenn ich es wollte. So kann ich einen viel kleineren und leichteren Laptopmitnehmen, wenn ich unterwegs bin.

Ein weiterer typischer Anwendungsfall für USB-Adapter ist das Nachrüsten bestimmter Anschlüsse bei älteren Geräten. Ein älterer Laptop kann dank eines USB-WLAN-Adapters 802.11ac nutzen oder mittels eines USB-Adapters Bluetooth verwenden.

Wichtig

Die CompTIA erwartet von Ihnen, dass Ihnen USB-Ethernet-Adapter vertraut sind.

23.3 Wartung und Pflege von tragbaren Computern

Die meisten tragbaren Computer sind ab Werk betriebsbereit und fertig konfiguriert. Aus der Sicht des Technikers besteht die Arbeit hauptsächlich in der Wartung und Pflege der tragbaren Computer. Hierzu gehören die Pflege der Akkus und die Verlängerung der Akkulaufzeit durch die richtigen Einstellungen in der Energieverwaltung, den Schutz der Geräte vor Verschmutzung und das Vermeiden von übermäßiger Wärme.

Alle Wartungsarbeiten für PCs müssen auch auf tragbaren Computern durchgeführt werden. Sie müssen Betriebssystem-Updates installieren und aktuelle, stabile Treiber verwenden. Verwenden Sie die entsprechenden Werkzeuge, um den einwandfreien Zustand der Speichergeräte zu überwachen und überflüssige Dateien zu entfernen. Sehen wir uns diese Aspekte nun einmal speziell für tragbare Computer an. Eine Besonderheit ist hier zu beachten: Da besonders kompakte Geräte oder Hybriden vom Aufbau oftmals Tablets oder Smartphones ähneln, sollten Sie gegebenenfalls auch den Hinweisen zur Fehlerbehebung in Kapitel 25, *Wartung und Pflege von mobilen Geräten*, folgen.

23.3.1 Akkus

Die Hersteller haben im Laufe der Jahre drei verschiedene Akkutypen für tragbare Computer verwendet: Nickel-Cadmium (Ni-Cd), Nickel-Metallhydrid (Ni-MH) und Lithium-Ionen (Li-Ion). Heutzutage finden nur noch Li-Ion-Akkus Verwendung, da diese die höchste Energiedichte pro Gewichtseinheit aufweisen und bei widrigen Umgebungsbedingungen weniger Probleme bereiten als die anderen Technologien.

Li-Ion (lithium-Ionen)

Li-Ion-Akkus (Lithium-Ionen) sind sehr leistungsstark und halten viel länger als die in den 1990er eingesetzten Ni-MH- und Ni-CD-Akkus. Der Nachteil von Li-Ion-Akkus ist, dass sie explodieren, wenn sie überladen oder durchbohrt werden – alle Li-Ion-Akkus verfügen daher über integrierte Schaltungen, die das versehentliche Überladen verhindern. Li-Ion-Akkus können nur in Geräten verwendet werden, die speziell dafür entwickelt wurden, und lassen sich nicht als Austauschakkus verwenden, um beispielsweise dem schönen alten Laptop aus dem Jahre 1998 wieder Leben einzuhauchen. Abbildung 23.18 zeigt einen typischen Li-Ion-Akku.



Abb. 23.18: Li-Ion-Akku

> **Hinweis**
>
> LiPo-Akkus (Lithium-Polymer-Akkus) sind eine Weiterentwicklung von Li-Ion-Akkus, bei denen eine der wesentlichen Komponenten einer Batterie, der Elektrolyt, nicht flüssig ist, sondern durch einen Elektrolyten auf Polymerbasis ersetzt wird, der als feste oder geleeartige Folie vorliegt. Dadurch ist man bei der Formgebung des Akkus nicht mehr auf die herkömmlichen Zylinder oder Quader beschränkt und kann, insbesondere bei kleinen Geräten, den vorhandenen Raum besser nutzen. Im Bereich tragbarer Compu-

ter haben LiPo-Akkus Li-Ion-Akkus noch nicht flächendeckend verdrängt, sie werden aber in vielen kleineren Geräten wie Tablets, Smartphones, tragbaren Geräten zur Medienwiedergabe und besonders kompakten Computern wie Hybriden und Ultrabooks (besonders dünne und leichte Notebooks) bevorzugt eingesetzt.

Pflege und Wartung von Akkus

Beachten Sie hier die folgenden allgemeinen Grundregeln: Lagern Sie Akkus immer kühl. Der Kühlschrank wäre zwar prinzipiell gut geeignet, kommt aber wegen der Feuchtigkeit, der Metallteile und der darin aufbewahrten Lebensmittel eher nicht infrage. Sorgen Sie zweitens dafür, dass die Akkus zu wenigstens 70–80% geladen sind. Entladen Sie drittens die Akkus niemals vollständig, es sei denn, Sie müssen das im Rahmen einer Kalibrierung tun. (Dabei setzen Sie den Akku im Wesentlichen gemäß einer schrittweisen Anleitung des Herstellers zurück.) Akkus vertragen nur eine begrenzte Zahl von Ladezyklen, bevor die Gesamtleistung nachlässt. Viertens, lassen Sie die Finger von beschädigten oder aufgeplatzten Akkus, denn die verwendeten Chemikalien sind sehr gefährlich und leicht entzündlich. (Sehen Sie sich auf YouTube an, was passiert, wenn ein Li-Ion- oder ein LiPo-Akku durchbohrt wird.) Und schließlich sollten Sie ausrangierte Akkus grundsätzlich recyceln lassen.

Tipp: Recycling alter Akkus

Liegt bei Ihnen noch ein alter Akku eines tragbaren PCs herum? Sie müssen ihn irgendwie loswerden, und weil solch ein Akku häufig sehr gefährliche Chemikalien enthält, können Sie ihn auch nicht einfach in den Hausmüll werfen. Früher oder später müssen Sie sich um das Problem kümmern. Unternehmen Sie Folgendes:

1. Suchen Sie im Internet nach einer nahegelegenen Batteriesammelstelle. Viele Händler, die selbst Batterien oder batteriebetriebene Geräte verkaufen, nehmen diese auch (in haushaltsüblichen Mengen) zurück.
2. In manchen Fällen können Sie alte Akkus bei Autozubehörhändlern loswerden, die alte Autobatterien entsorgen. Hört sich merkwürdig an, stimmt aber! Sehen Sie sich nach solch einem Händler in Ihrer Nähe um.
3. In vielen Städten gibt es Sammelstellen für gefährliche Substanzen oder Recyclingdienste. Zumindest sollte man Ihnen hier hinsichtlich der Akkuentsorgung weiterhelfen können.

23.3.2 Energieverwaltung

Der typische Laptop enthält zahlreiche Bauteile, die alle Energie benötigen. Bei den frühen Laptops bestand ein großes Problem darin, dass diese einzelnen Bauteile kontinuierlich Energie verbrauchten, und zwar unabhängig davon, ob das jeweilige Gerät gerade benötigt wurde oder nicht. Auch wenn es keine Zugriffe gab, drehte sich so z.B. unablässig die Festplatte, die CPU wurde so schnell wie möglich getaktet, ob wohl es kaum etwas zu berechnen gab, und der LCD-Monitor war in Betrieb, auch wenn der Benutzer nicht vor dem Gerät saß.

Im Laufe der Jahre wurde viel Arbeit in die Verbesserung der Akkulaufzeit mobiler Geräte investiert. Es wurden bessere Akkus und energiesparendere Komponenten entwickelt, aber auch die Firmware des Systems und die Firmware einzelner Bauteile arbeiten zusammen, um den Energieverbrauch zu regeln. Um de Energieverbrauch zu senken, kann der Computer nicht genutzte Komponenten abschalten, bis sie benötigt werden, und in einen Ruhezustand übergehen, wenn das Gerät nicht verwendet wird, und die Leistung energiehungriger Komponenten wie der CPU drosseln, um sie an die tatsächliche Arbeitslast anzupassen. Die gesamte Steuerung der Hardware, des BIOS und des Betriebssystems zur Verringerung der Leistungsaufnahme ist unter der Bezeichnung *Energieverwaltung* bekannt.

Energiesparmodi

Wenn man nicht weiß, was hinter den Kulissen vor sich geht, dann scheint ein Computer eindeutig ein- oder ausgeschaltet zu sein. Tatsächlich verbrauchen die meisten Computer (sowohl Desktops als auch Laptops!), die offenbar ausgeschaltet sind, zumindest ein wenig Energie und befinden sich in einem Energiesparmodus. Die CompTIA konzentriert sich auf die grundlegenden Optionen der Energieverwaltung in der Systemsteuerung, es kann aber nicht schaden, die verschiedenen Energiesparmodi zu kennen.

Hinweis

Die Bezeichnungen für Energiesparmodi sind vom Betriebssystem abhängig und ändern sich manchmal sogar von Version zu Version, die grundlegenden Konzepte sind jedoch dieselben.

Wenn der Computer ausgeschaltet ist, fährt er das Betriebssystem nach dem Einschalten komplett neu hoch. Es gibt zwei Modi, in denen sich ein ausgeschalteter Computer befinden kann:

- **Mechanical-Off-Modus**: Das System und sämtliche Komponenten (mit Ausnahme der Echtzeituhr) sind tatsächlich ausgeschaltet.
- **Softpower-Off-Modus**: Das System ist weitgehend ausgeschaltet, bis auf die Komponenten, die von Tastatur, LAN oder USB-Geräten benötigt werden, um es aufzuwecken.

Scheinbar ausgeschaltete Computer können sich im Energiesparmodus (oder Standby-Modus) befinden. Wenn sie aufgeweckt werden, sind alle Programme, Prozesse und geöffneten Fenster wieder aktiv, die zum Zeitpunkt liefen, als das System in den Energiesparmodus versetzt wurde. Es gibt ein paar feine Unterschiede zwischen den verschiedenen Energiesparmodi, aber wichtig ist vor allem:

- Ein Gerät im Energiesparmodus kann schnell wieder aufgeweckt werden, weil der Arbeitsspeicher nicht abgeschaltet wird. Das ermöglicht es dem System, seinen Zustand zu speichern. Wenn es zu einer unerwarteten Unterbrechung der Stromversorgung kommt, können die Daten im RAM verloren gehen.
- Geräte im erweiterten Energiesparmodus, dem sogenannten *Ruhezustand*, brauchen zum Aufwachen länger, weil sie vor dem Ausschalten den Inhalt des Arbeitsspeichers auf der Festplatte speichern, und die Wiederherstellung dauert einen Moment. Der Ruhezustand hat jedoch die Vorteile, dass er mehr Energie spart und dass keine Daten verloren gehen, wenn es zu einer Unterbrechung der Stromversorgung kommen sollte.
- Konfiguration der Energieverwaltung

Die Energieverwaltung lässt sich über die BIOS-Einstellungen oder vom Betriebssystem aus konfigurieren. Die Einstellungen des Betriebssystems haben dabei Vorrang vor den BIOS-Einstellungen. Auch wenn sich die Implementierungen unterscheiden, gibt es bei der BIOS-Konfiguration einige allgemein übliche Einstellungen, wie die Möglichkeit, die Energieverwaltung zu aktivieren oder zu deaktivieren, festzulegen, welche Geräte das System aufwecken dürfen, zu konfigurieren, wie sich der Netzschalter verhält, oder anzugeben, wie sich das System verhalten soll, wenn es nach einem Stromausfall wieder mit Spannung versorgt wird.

In den Betriebssystemen erscheinen verständliche Begriffe, wie *Energieverwaltung* oder *Energie sparen*, aber in manchen Hilfsprogrammen könnten Ihnen auch eher technische Ausdrücke begegnen. Wenn Sie die Einstellungen nicht unter einer offensichtlichen Bezeichnung finden können, sind sie vielleicht nach der 1992 von Intel entwickelten *APM*-Spezifikation (*Advanced Power Management*) benannt, der 1996 der *ACPI*-Standard (*Advanced Configuration and Power Interface*) folgte.

In vielen BIOS-Versionen lassen sich außerdem die Aufwachereignisse über entsprechende Einstellungen so definieren, dass z.B. ein Netzwerkadapter überwacht wird (Abbildung 23.19). Diese Funktion finden Sie unter Bezeichnungen wie z.B. *Wake on LAN* im BIOS-Setup. Abbildung 23.20 zeigt ein typisches modernes BIOS mit derartigen Einstellungen.

```
Phoenix - AwardBIOS CMOS Utility
Power

APM Configuration                                  Select Menu

Restore on AC Power Loss         [Power-Off]       Item Specific Help▶▶
PWR Button < 4 secs              [Instant-Off]
Power Up On PCI/PCIE Devices     [Disabled]        Set the Data, Time
USB Resume from S5               [Disabled]        resume by Alarm.
Power On By RTC Alarm            [Enabled]
Date(of Month) Alarm             [ 5]
Alarm Time(hh:mm)                  2 :  9 :  5
Power Up By PS/2 Mouse           [Disabled]
Power Up By PS/2 Keyboard        [Disabled]

F1:Help    ↑↓:Select Item    -/+: Change Value       F5:Setup Defaults
ESC:Exit   ▶◀:Select Menu    Enter: Select SubMenu   F10:Save and Exit
```

Abb. 23.19: Einrichtung eines Aufwachereignisses im BIOS

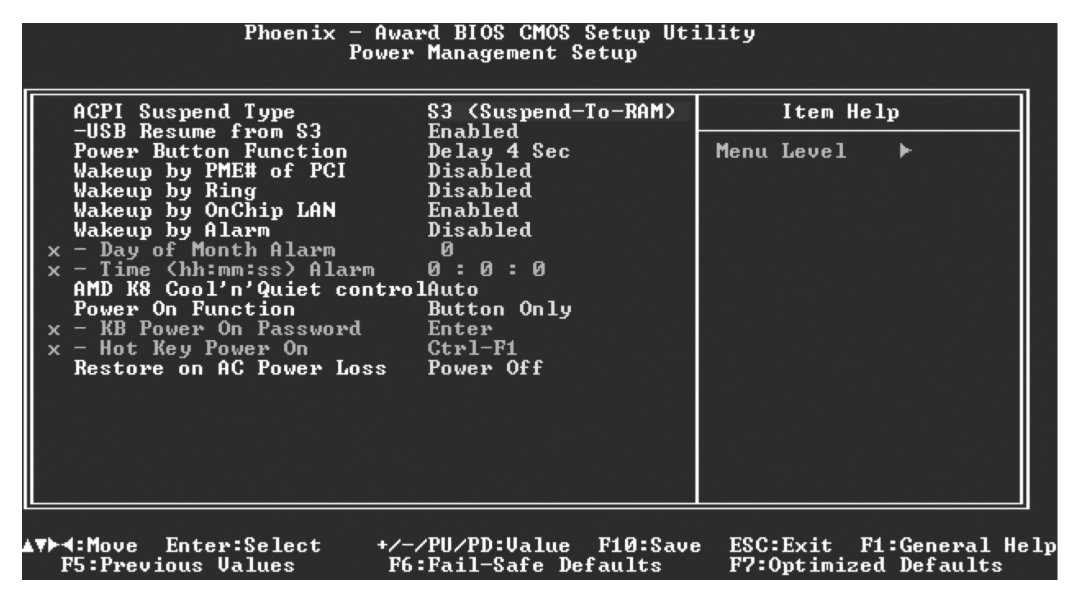


Abb. 23.20: BIOS mit Optionen zur ACPI-Einrichtung

In Windows finden Sie die APM/ACPI-Einstellungen im Applet ENERGIEOPTIONEN der Systemsteuerung oder in Windows 10 in der Einstellungen-App im Bereich SYSTEM|NETZBETRIEB UND ENERGIESPAREN. Windows bietet verschiedene vordefinierte Energiesparpläne wie AUSBALANCIERT, ENERGIESPARMODUS oder HÖCHSTLEISTUNG an (Abbildung 23.21). Sie können z.B. einen Energiesparplan für Ihren Laptop anpassen und die Anzeige bei Akku- oder Netzbetrieb nach einer bestimmten Zeitspanne abschalten lassen und den Rechner entsprechend den eigenen Vorstellungen in den Schlafmodus schicken (Abbildung 23.22). Klicken Sie auf ZUSÄTZLICHE ENERGIEEINSTELLUNGEN, um die Energiesparpläne anzuzeigen. Dort können Sie viele weitere Einstellungen vornehmen, beispielsweise für den Ruhezustand (Abbildung 23.23).

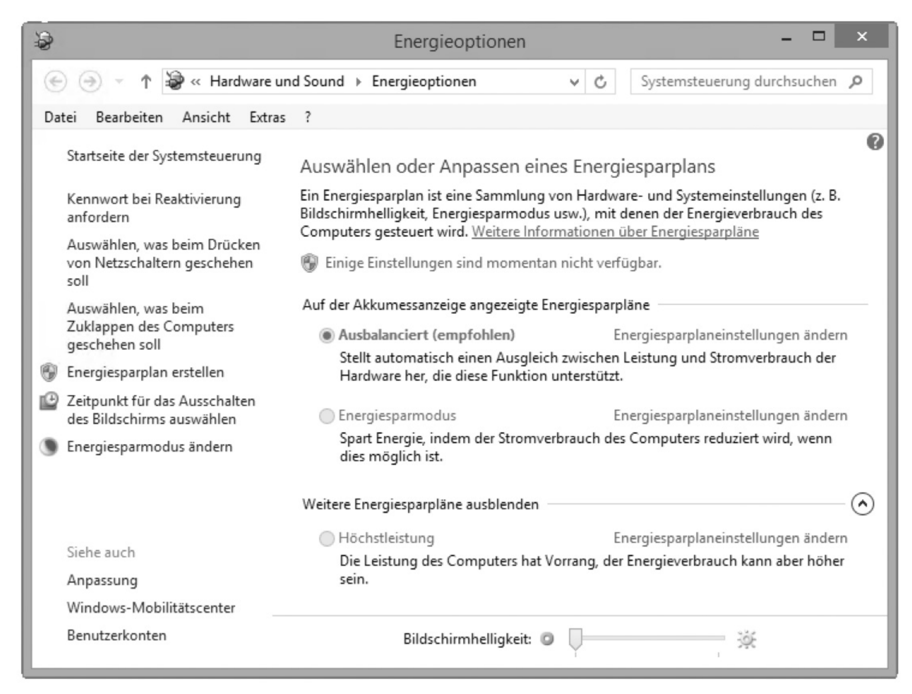


Abb. 23.21: Energiesparpläne in Windows 8.1

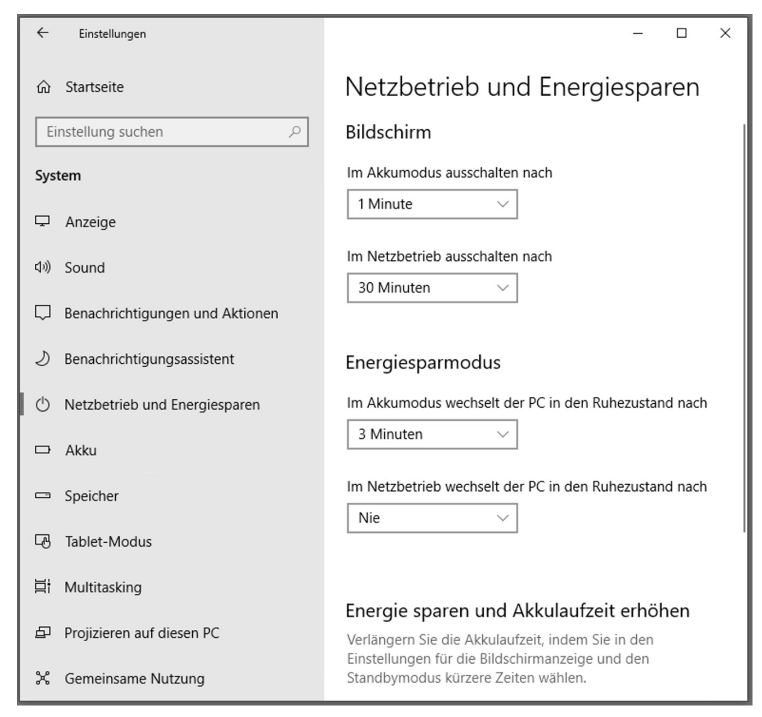


Abb. 23.22: Anpassung eines Energiesparplans für ein Notebook in Windows 10

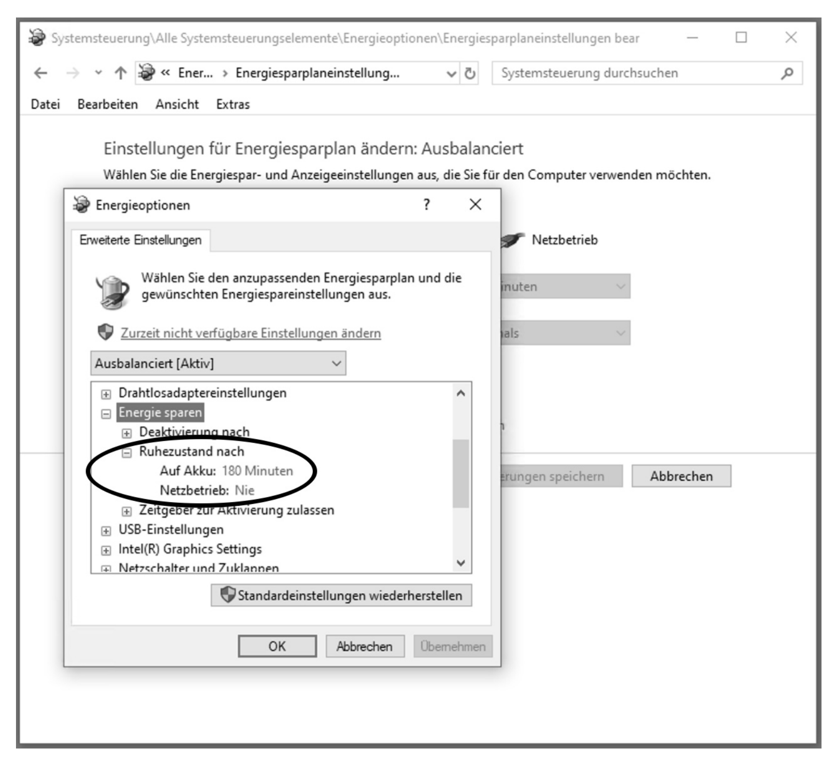


Abb. 23.23: Einstellungen für den Ruhezustand in Windows 10

Tipp: Anpassen der Energieoptionen

Öffnen Sie das Applet ENERGIEOPTIONEN und sehen Sie sich die verschiedenen Einstellungen an. Welchen Energiesparplan verwendet Ihr Computer derzeit? Prüfen Sie, ob er im Modus AUSBALANCIERT oder HÖCHSTLEISTUNG läuft. Ändern Sie ihn auf ENERGIESPARMODUS, falls Letzteres der Fall ist und klicken Sie auf ENERGIESPARPLANEINSTELLUNGEN ÄNDERN. Machen Sie sich auch mit den erweiterten Energieeinstellungen vertraut, indem Sie auf ERWEITERTE ENERGIEEINSTELLUNGEN ÄNDERN klicken.

Probieren Sie aus, einige der verschiedenen Einstellungen für die verschiedenen Energiesparpläne anzupassen. Ändern Sie beispielsweise den Wert für den Eintrag BILDSCHIRM AUSSCHALTEN NACH auf 5 Minuten. Keine Sorge: Sie können nichts kaputt machen, wenn Sie mit diesen Einstellungen herumspielen.

Beachten Sie auch, dass Microsoft in Windows 10 die Voreinstellung für Laptops auf AUSBALANCIERT geändert hat. Sie können das aber jederzeit in den erweiterten Energieeinstellungen ändern.

Manuelle Energieverwaltung

Die meisten Notebooks bieten die Möglichkeit, unter bestimmten Umständen den Energieverbrauch durch manuelle Maßnahmen zu senken. Die Hardware-Schalter oder Tastenkombinationen zum Abschalten von WLAN und Bluetooth wurden bereits erwähnt. Viele neuere Notebooks haben ein Feature von Smartphones und Tablets übernommen, das die meisten oder alle drahtlosen Dienste gleichzeitig deaktiviert: den *Flugmodus*. Neben der eigentlich beabsichtigten Anwendung ist der Flugmodus auch äußerst praktisch, um mehrere energiehungrige Komponenten schnell gleichzeitig abzuschalten.

Bei Laptops mit Tastaturbeleuchtung gibt es immer auch die Option, diese abzuschalten, wenn sie nicht benötigt wird. Hierfür gibt es meist eine weitere Tastenkombination. Durch das Verringern der Bildschirmhelligkeit lassen sich ebenfalls noch ein paar Minuten wertvoller Akkulaufzeit herauskit-

zeln. In Abbildung 23.24 sehen Sie die Tasten, die in Kombination mit FN zur Anpassung der Bildschirmhelligkeit dienen.

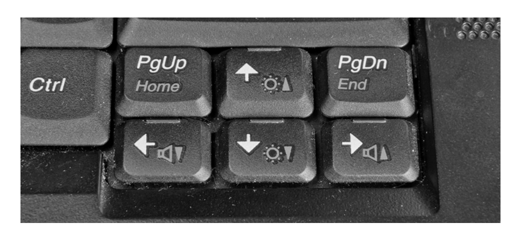


Abb. 23.24: Tasten zur Anpassung der Helligkeit

Eine der besten Methoden, unterwegs Energie zu sparen, ist eine sorgfältige Planung. In der Praxis bedeutet das, die Anzahl der Dateien und Geräte zu minimieren, die man verwendet, während der Laptop mit dem Akku betrieben wird. Wenn ich beispielsweise verreisen muss und mir vorab klar ist, dass ich einige auf dem Dateiserver befindliche Daten benötige, kopiere ich diese auf mein Notebook, solange ich noch in der Nähe einer Steckdose bin. Man ist natürlich versucht, die Daten stattdessen auf einen USB-Speicherstick zu kopieren, um sich das Hochfahren des Laptops zu sparen oder die Synchronisierung via Dropbox zu verwenden, aber sowohl die Verwendung von WLAN als auch die Nutzung des USB-Speichersticks verbrauchen unterwegs unnötig Energie.

Unter Windows kann ich die benötigten Dateien sogar als *Offlinedateien* kennzeichnen, sodass auf meiner Festplatte eine lokale Kopie gespeichert wird. Wenn mein Laptop mit dem Netzwerk im Büro verbunden ist, werden die so markierten Dateien und Ordner automatisch mit denen auf dem Server synchronisiert. Alle Änderungen, die ich unterwegs durchgeführt habe, werden dann auf den Server übertragen und alle Änderungen, die sonst jemand auf dem Server vorgenommen hat, landen auf meinem Laptop. (Falls auf beiden Seiten Änderungen stattgefunden haben, erscheint eine Meldung, dass es einen Konflikt gibt, sodass Sie dieses Problem lösen können, ohne Gefahr zu laufen, irgendwelche wichtigen Daten zu überschreiben.)

Klicken Sie mit der rechten Maustaste auf einen Ordner und wählen Sie IMMER OFFLINE VERFÜGBAR, um diesen Ordner und seinen Inhalt als Offlinedateien zu kennzeichnen. Die Synchronisierung wird durchgeführt, und das war's. Wenn Sie die Dateien unterwegs öffnen möchten, öffnen Sie in der Systemsteuerung das Applet SYNCHRONISIERUNGSCENTER (Abbildung 23.25) und klicken Sie in der Aufgabenliste auf OFFLINEDATEIEN VERWALTEN. Hier können Sie auf die Daten zugreifen (Abbildung 23.26). Klicken Sie auf OFFLINEDATEIEN ANZEIGEN, um an Ihre Dateien zu gelangen.

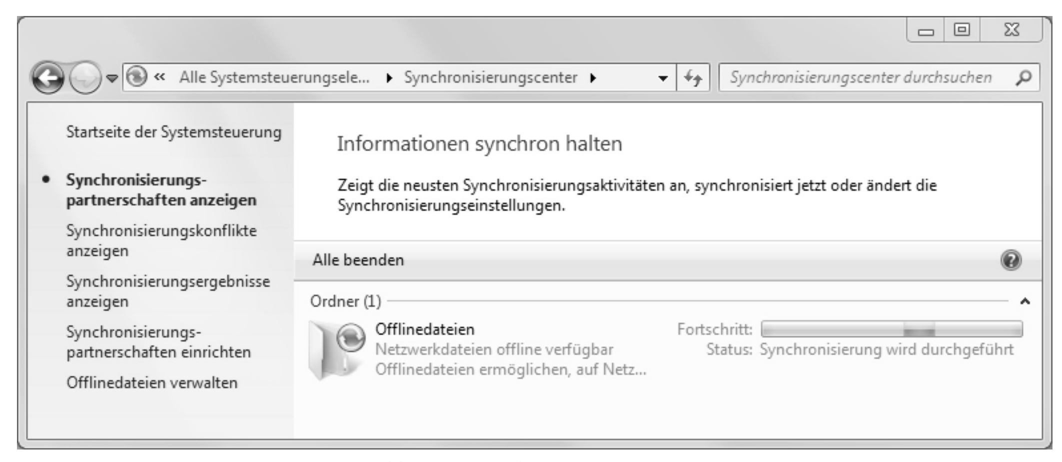


Abb. 23.25: Synchronisierungscenter

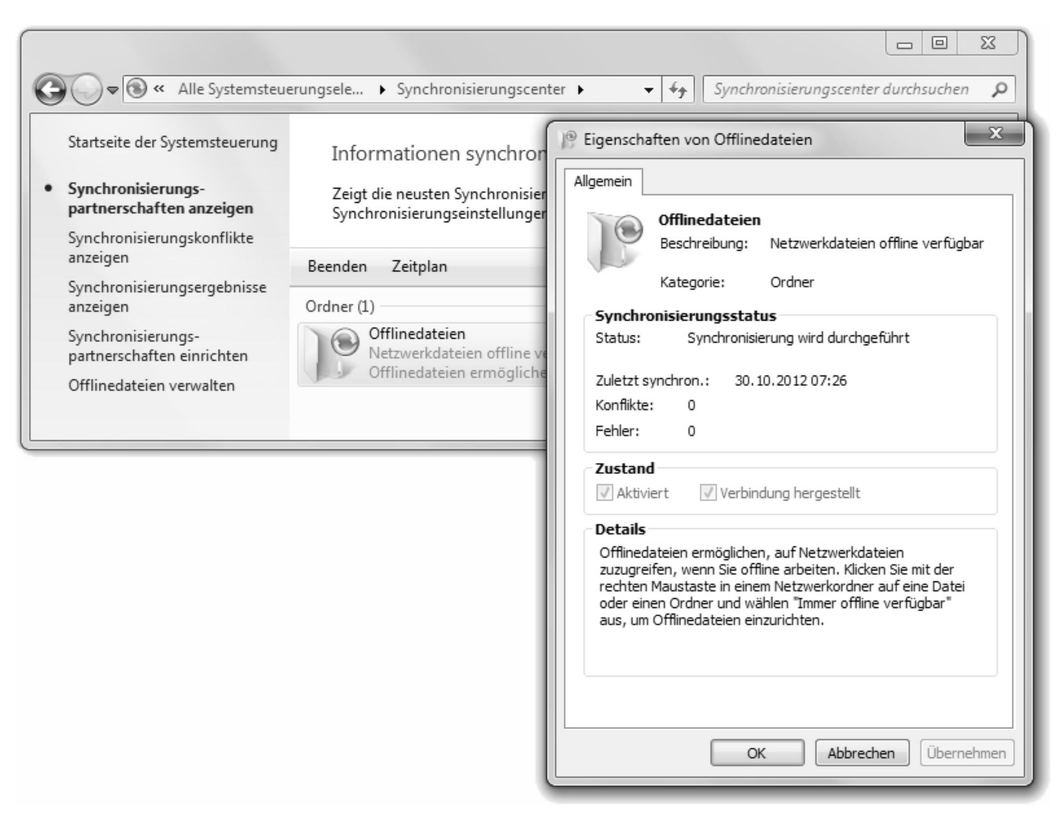


Abb. 23.26: Das Dialogfeld EIGENSCHAFTEN VON OFFLINEDATEIEN

Wichtig

Weitere Möglichkeiten, die Betriebsdauer zu verlängern, sind der Einsatz eines Ersatzakkus oder die Verwendung einer sogenannten *Powerbank* zum Nachladen des Akkus, falls dieser nicht austauschbar ist.

23.3.3 Reinigung

Die meisten tragbaren Computer werden deutlich schlechter als durchschnittliche Desktop-Rechner behandelt. Wenn Sie keine besonderen Vorkehrungen treffen, kann die Lebensdauer eines tragbaren Computers durch ständigen Gebrauch, Reisen, Speisereste und anderes mehr als deutlich verkürzt werden. Eine der wichtigsten Maßnahmen besteht darin, den Laptop regelmäßig zu reinigen. Verwenden Sie einen geeigneten Bildschirmreiniger (keinesfalls Glasreinigungsmittel!), um Fingerabdrücke und Staub vom empfindlichen LCD-Bildschirm zu entfernen. Näheres dazu erfahren Sie in Kapitel 17, *Anzeige: Bildschirm und Grafikkarte*.

In Kapitel 27 sehen wir uns Bedrohungen durch Umweltbedingungen näher an, aber wenn Sie den Computer in einer staubigen oder schmutzigen Umgebung betrieben haben, sodass allein schon die Luftqualität Probleme verursacht, ist Druckluftspray hervorragend geeignet, um Staub und Krümel von der Tastatur zu entfernen und die Anschlüsse sauber zu halten. Verwenden Sie kein Wasser zur Reinigung der Tastatur! Schon geringe Feuchtigkeitsmengen im Innern des tragbaren Computers können Bauteile zerstören.

23.3.4 Wärmeentwicklung

Bei der Wartung und Pflege eines intakten tragbaren PC müssen Sie dem Problem der Wärmeentwicklung einige Aufmerksamkeit schenken. Jeder tragbare Computer enthält zahlreiche eng beieinanderliegende elektronische Komponenten. Anders als in ihren großen Brüdern bleibt in Laptops nicht gerade viel Platz für die freie Luftzirkulation, die Lüftern eine gute Kühlung ermöglichen würde. Obwohl alle Komponenten im Innern des tragbaren Computers relativ wenig Energie verbrauchen, erzeugen sie trotz allem gemeinsam immer noch eine ganze Menge Wärme. Zu hohe Temperaturen können aber Systemabstürze und Hardwaredefekte verursachen. Achten Sie also besonders auf diesen Aspekt. Dazu die folgenden Hinweise:

- Verwenden Sie die Energieverwaltung auch dann, wenn Sie mit Netzstrom arbeiten. Dies ist insbesondere dann wichtig, falls Sie in einem warmen Raum (mehr als 25 Grad) arbeiten.
- Achten Sie auf Spielraum zur Luftzirkulation zwischen dem Laptop und der Oberfläche, auf der er steht. Ganz ungünstig wäre es, wenn Sie ihn auf ein Kissen in Ihrem Schoß legen, denn das sorgt garantiert für einen Wärmestau! Benutzen Sie immer eine harte, glatte Stellfläche.
- Verwenden Sie einen Tastaturschutz nicht über einen längeren Zeitraum.
- Achten Sie auf den laufenden Lüfter (sofern Ihr Laptop über einen solchen verfügt). Wenn er öfter sehr schnell läuft (Sie erkennen das am surrenden Geräusch), sollten Sie die Einstellungen in der Energieverwaltung und das Arbeitsumfeld prüfen. Sorgen Sie dafür, dass die Ursachen der übermäßigen Wärmeentwicklungen beseitigt werden.
- Und da wir gerade bei Lüftern sind, sollten Sie natürlich sofort alarmiert sein, wenn es plötzlich gar kein Lüftergeräusch mehr gibt. Lüfter können ausfallen, woraufhin der Laptop überhitzt und abstürzt.

23.3.5 Den Computer schützen

Der Preis einfacher Laptops sinkt weiterhin, auch wenn wirklich leistungsfähige Systeme immer noch teuer sind. Um Ihre Investition zu schützen, sollten Sie sich an bestimmte Regeln halten. Sie haben in diesem Kapitel bereits Tipps zur Reinigung und zur Wärmeentwicklung gelesen, hier soll es nun um die Portabilität der tragbaren Computer gehen.

Stolpern

Achten Sie beim Anschließen des Laptops an eine Steckdose darauf, wie Sie das Netzkabel verlegen. Eine der Hauptursachen für zerstörte Laptops ist, dass jemand über das Netzkabel stolpert und den Laptop vom Tisch reißt. Das ist insbesondere dann der Fall, wenn Sie irgendwo eine öffentlich zugängliche Steckdose benutzen, wie z.B. in einem Café oder am Flughafen. Denken Sie daran, denn damit könnten Sie Ihrem tragbaren Begleiter das Leben retten!

Aufbewahrung

Wenn Ihr Laptop längere Zeit nicht benutzt wird, kann die sorgfältige Aufbewahrung dafür sorgen, dass er auch noch funktioniert, wenn Sie ihn wieder einschalten. Sie sollten in eine qualitativ hochwertige Notebook-Tasche investieren, die ausreichend gepolstert sein sollte. Damit schützen Sie Ihr System nicht nur im Alltag auf dem Weg von zu Hause ins Büro, sondern sorgen auch dafür, dass es vor Staub und Tierhaaren geschützt wird. Wenn Sie das Gerät längere Zeit nicht benutzen, sollten Sie außerdem den Akku entnehmen, sofern das möglich ist. Ob der Akku nun entnehmbar ist oder nicht, er sollte zum Teil geladen sein und gelegentlich nachgeladen werden, um eine vollständige Entladung zu verhindern.

Reisen

Wenn Sie mit einem Laptop reisen, achten Sie darauf, sich vor Diebstahl zu schützen. Verwenden Sie möglichst eine Tasche, die nicht nach Computer aussieht. Ein gut gepolsterter Rucksack ist ein wun-

derbares Transportmittel für einen Laptop und außerdem weniger attraktiv für Diebe, auch wenn es bei manchen Marken oder Typen ziemlich offensichtlich ist, dass sie zum Transport von Computern dienen. Kleinere Geräte wie Ultrabooks können oft in weniger auffälligen Taschen verstaut werden. Vergessen Sie nicht, möglicherweise benötigtes Zubehör mit einzupacken, wie z.B. modulare Geräte, Ersatzakkus und Netzteile. Entfernen Sie optische Medien aus den Laufwerken. Und vor allem: Sichern Sie alle wichtigen Daten, bevor Sie sich auf den Weg machen.

Vergewissern Sie sich, dass der Akku nicht ganz entladen ist. Aufgrund der erhöhten Sicherheitsmaßnahmen auf Flughäfen müssen Sie Ihren Rechner möglicherweise einschalten, um zu beweisen, dass es sich wirklich um einen Computer handelt und nicht um einen Transportbehälter für fragwürdige Materialien. Und lassen Sie Ihren Laptop nie aus den Augen. Wenn er durchleuchtet werden soll, bitten Sie um eine manuelle Durchsuchung. Die Röntgenstrahlen können Ihrem Rechner zwar im Unterschied zu einem Metalldetektor nicht schaden, aber wenn der Laptop vor Ihnen durch die Sicherheitsschleuse gelangt, könnte ihn jemand stehlen. Wenn Sie mit dem Flugzeug reisen, verstauen Sie den Laptop am besten unter dem Sitz Ihres Vordermanns, um ihn im Auge behalten zu können.

Wenn Sie ins Ausland reisen, müssen Sie beim Anschluss an das Stromnetz aufpassen. Nordamerika verwendet Netzspannungen von etwa 115 V, ansonsten wird überwiegend 230 V verwendet. Die Netzteile vieler tragbaren Computer können sich automatisch an die jeweilige Spannung anpassen. Bei einem solchen Netzteil ist irgendwo angegeben, mit welcher Eingangs- und Ausgangsspannung es arbeitet (Abbildung 23.27). Vergewissern Sie sich besser doppelt, dass das Netzteil für die Spannung geeignet ist, die in dem Land verwendet wird, das Sie bereisen. Ist das nicht der Fall, dann benötigen Sie einen Spannungswandler, den Sie in Elektrofachgeschäften kaufen können.



Abb. 23.27: Eingangs- und Ausgangsspannung eines Netzteils

Versand

Ein Großteil der Ratschläge für das Aufbewahren und Reisen gilt auch für den Versand. Entnehmen Sie nach Möglichkeit den Akku und entfernen Sie Datenträger aus den Laufwerken. Verpacken Sie den Computer gut und tarnen Sie den Behälter möglichst gut. Sichern Sie alle Daten und achten Sie auf die Garantiebedingungen. Nutzen Sie für den Versand vertrauenswürdige Transportunternehmen und fragen Sie immer nach einer Versandnummer und möglichst nach einer Empfangsbestätigung. Außerdem ist eine Transportversicherung empfehlenswert. Und wenn Sie der Angestellte fragt, was sich in dem Behälter befindet, erzählen Sie besser etwas von »Elektrogeräten« und sprechen nicht von »ein neuer Laptop mit 20-Zoll-Bildschirm«.

Sicherheit

Wenn jemand Ihren Laptop wirklich stehlen will, dann findet er auch einen Weg. Es gibt jedoch Möglichkeiten, sich selbst und die eigenen Geräte zu weniger attraktiven Angriffszielen zu machen. Wie Sie bereits erfahren haben, kann Tarnung nie schaden.

Ein weiteres physisches Hemmnis ist ein Laptop-Schloss. Vergleichbar mit einem Fahrradschloss hat es eine Schlinge an dem einen Ende und ein Schloss am anderen. Dabei geht es darum, dass Sie die

Schlinge um einen festen Gegenstand (z.B. einen Bettrahmen) legen und dann Ihren Laptop daran befestigen können (Abbildung 23.28). Auch hier gilt: Wenn jemand Ihren Laptop stehlen will, findet er einen Weg. Im Zweifelsfall demontiert er den Bettrahmen. Am besten schützen Sie sich, wenn Sie wachsam bleiben und den Rechner nicht aus den Augen lassen.

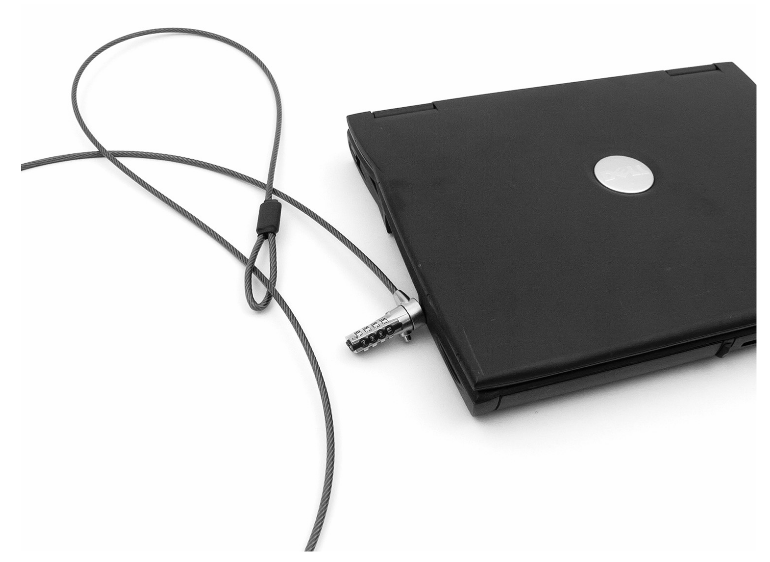


Abb. 23.28: Notebook mit angeschlossenem Sicherungskabel

Eine Alternative zur physischen Sicherung eines Laptops mit einem Schloss ist die Verwendung eines Software-Verfolgungssystems, das GPS-Signale nutzt. Es verhindert zwar nicht, dass ihr Gerät gestohlen wird, kann aber dank der Netzwerkfähigkeiten und der vielen in aktuellen Geräten vorhandenen Sensoren dabei helfen, es wiederzufinden. Die genaue Funktionalität hängt zwar von der jeweiligen Software ab, aber typischerweise können Sie sich den Aufenthaltsort des gestohlenen Computers anzeigen lassen, Fotos oder Audio aufnehmen und sensible Daten löschen. Da diese Funktionalität vor allem bei Smartphones und Tablets vorhanden ist, hebe ich mir dieses Thema für Kapitel 25 auf.

23.4 Aufrüstung und Reparatur von tragbaren Computern

Ein kompetenter Techniker ist bis zu einem gewissen Grad durchaus in der Lage, einen tragbaren Computer aufzurüsten oder zu reparieren, wahre Notebook-Techniker sind allerdings Spezialisten. Zur Aufrüstung der grundlegenden Komponenten kommt man für gewöhnlich nicht darum herum, den guten alten Schraubendreher hervorzuholen und natürlich auf elektrostatische Entladungen achtzugeben. Um defekte tragbare Computer erfolgreich zu *reparieren*, sind hingegen sorgfältige Vorbereitung, Geduld, spezielle Werkzeuge und Dokumentation erforderlich. Und eine wirklich ruhige Hand ist ebenfalls vonnöten. Dieser Abschnitt gibt einen Überblick über die Aufrüstung und Reparatur. Beachten Sie jedoch, dass es hier aufgrund der wachsenden Zahl von Formfaktoren und der immer kleineren Geräte viele Ausnahmen gibt, insbesondere dann, wenn es um besonders kompakte Modelle geht. Solche Geräte auseinanderzunehmen, ist oft sehr schwierig, und die Bauteile sind möglicherweise verlötet oder verwenden herstellerspezifische Anschlüsse.

23.4.1 Auseinandernehmen des Geräts

Das Auseinandernehmen eines tragbaren Computers ist für gewöhnlich ganz einfach, wenn vom Hersteller vorgesehen ist, dass der Endkunde selbst Hand anlegt. Die wahre Kunst besteht daran, ihn wie-

der so zusammenzubauen, dass er auch funktioniert! Beachten Sie beim Auseinandernehmen und Zusammenbau die folgenden Punkte:

- *Notieren Sie sich die Position aller Kabel und Schrauben und kennzeichnen oder etikettieren Sie diese.* In Laptops werden keine Standardanschlüsse und gewöhnliche Schrauben verwendet. Ihnen werden die seltsamsten Schraubentypen begegnen. Der Versuch, eine Schraube in ein unpassendes Gewinde einzuschrauben, kann zur Beschädigung der Schraube, des Gewindes oder einer am falschen Platz verkeilten oder verkanteten Schraube führen.
- *Sortieren Sie alle dem Gerät entnommenen Bauteile aufs Sorgfältigste.* Ganz im Ernst: Breiten Sie auf Ihrer Arbeitsfläche ein großes weißes Blatt Bastelpapier aus, legen Sie die entnommenen Bauteile in sinnvoller Reihenfolge darauf ab und notieren Sie daneben, wo die Komponenten hingehören und gegebenenfalls, womit sie verbunden sind. Verwenden Sie gegebenenfalls die Kamera Ihres Smartphones oder eine Webcam, um Aufnahmen der Position von Bauteilen zu machen, falls etwas verloren gehen sollte.
- *Nutzen Sie die Dokumentation des Herstellers.* Ich kann diesen Punkt gar nicht stark genug hervorheben. Im Gegensatz zu normalen Desktop-PCs ist der innere Aufbau eines Laptops nicht standardisiert. In einem tragbaren Computer ist alles so ausgelegt, dass es die Anforderungen des Herstellers in bestmöglicher Weise erfüllt. Es mag sein, dass zwei Modelle desselben Herstellers einen ähnlichen inneren Aufbau besitzen, sehr viel wahrscheinlicher ist es aber, dass sie sich deutlich voneinander unterscheiden.
- *Verwenden Sie ausschließlich das passende Handwerkzeug.* Insbesondere im Inneren eines tragbaren Computers werden Sie die merkwürdigsten, winzigen Schrauben vorfinden, die Sie ohne spezielle Kreuzschlitz- oder Torx-Schraubendreher nicht lösen oder anziehen können. Zum Aufhebeln mancher Komponenten sind kleine Spatel aus Metall oder Kunststoff nötig. Abbildung 23.29 zeigt ein Einsteiger-Set von Spezialwerkzeugen, das Sie bei `eustore.iFixit.com` erhalten (zu denen in Kürze noch Weiteres zu sagen ist). Die Profi-Version eines solchen Sets besteht aus mehr als 70 Werkzeugen, und weitere Werkzeuge nur zum Aufrüsten gibt es ebenfalls! Wie eingangs bereits erwähnt: Echte Laptop-Techniker sind Spezialisten.

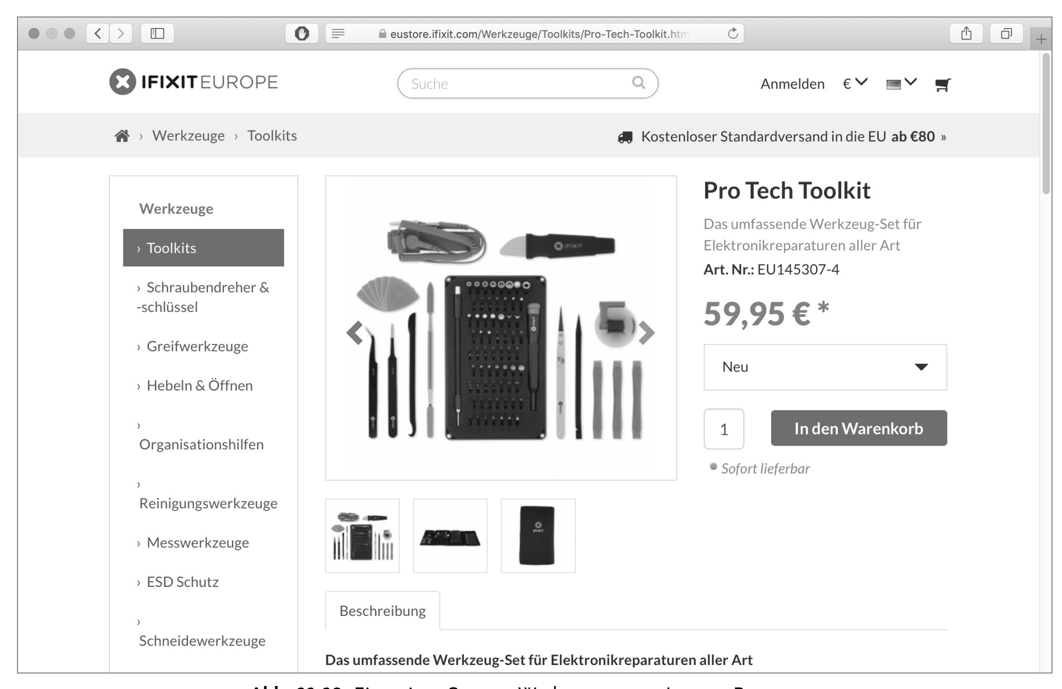


Abb. 23.29: Einsteiger-Set von Werkzeugen zur Laptop-Reparatur

Wichtig

Merken Sie sich für die CompTIA A+-Prüfung die vier Schritte beim Auseinandernehmen:

1. Dokumentieren und Kennzeichnen der Position von Kabeln und Schrauben
2. Sortieren der Bauteile
3. Herstellerdokumentation beachten
4. Geeignetes Werkzeug verwenden

Nun wissen Sie also, wie man beim Auseinandernehmen eines Geräts offiziell vorzugehen hat, daher muss ich eines klarstellen: Viele Hersteller gestatten es nicht jedem beliebigen Techniker, auf die Dokumentation zuzugreifen, sondern nur autorisierten Vertragshändlern. Was ist zu tun, wenn Sie sich nun einem unbekannten Notebook gegenübersehen, das Ihnen ein Kunde zur Reparatur gebracht hat?

Es gibt letztlich zwei Möglichkeiten. Sie können versuchen, einen Spezialisten zu finden und Ihren Kunden an diesen verweisen. Wenn das fragliche Gerät betriebsnotwendig ist und es sich um ein kompliziertes Problem handelt, ist das meist die beste Entscheidung. Wenn Sie das Problem selbst angehen möchten oder Sie glauben, damit fertig zu werden, sollten Sie auf zwei Quellen zurückgreifen: YouTube und `iFixit.com`.

Alle tragbaren Computer besitzen eine exakte Modellbezeichnung. Beschreiben Sie bei der YouTube-Suche möglichst genau, was Sie zu tun beabsichtigen, wie z.B. »Tastatur eines Dell Inspiron 5567 austauschen«, und sehen Sie sich das Ergebnis an (Abbildung 23.30). Es wird Sie wahrscheinlich erstaunen, insbesondere wenn das Gerät schon ein paar Jahre alt ist. Wenn es um defekte Geräte geht, sind Sie auf der Welt wahrhaftig nicht allein.

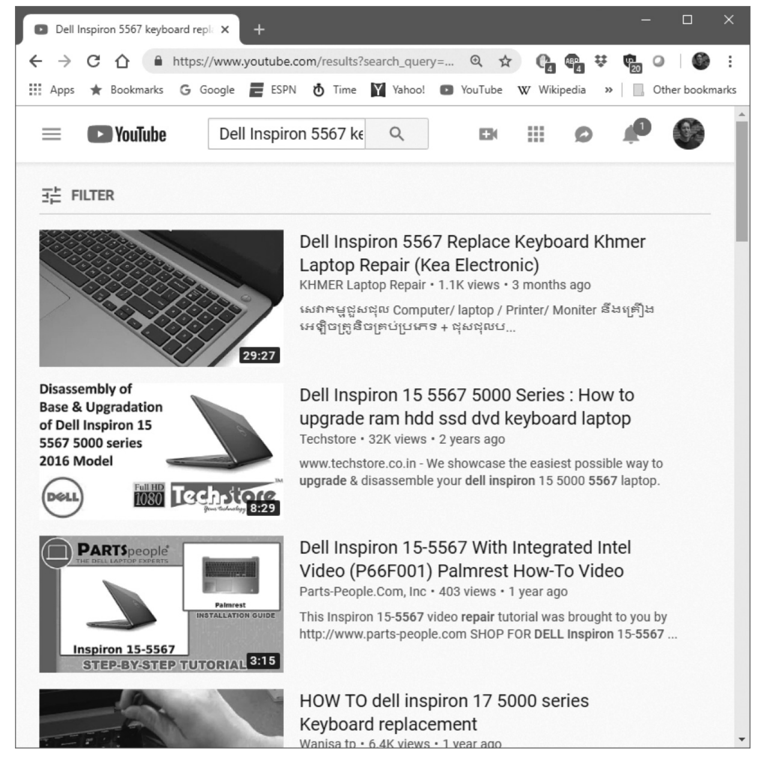


Abb. 23.30: YouTube Suchergebnisse

Sobald Sie das entsprechende Video, oder eines, das Ihrem Problem hinreichend nahe kommt, gefunden haben, sehen Sie es sich an. Wenn es Ihnen zu schwierig erscheint oder teures Spezialwerkzeug erforderlich ist, verweisen Sie Ihren Kunden doch besser an einen Spezialisten. Versuchen Sie ansonsten herauszufinden, welche Werkzeuge und Bauteile Sie benötigen. Modellspezifische Bauteile (wie etwa die Dell-Tastatur im vorhergehenden Beispiel) erhalten Sie meist nur über den Hersteller. Gebräuchlichere Komponenten wie Festplatten, CPUs usw. bekommen Sie auch im einschlägigen Fachhandel.

Hinsichtlich allgemeiner Werkzeuge, Bauteile und sehr ausführlichen, bebilderten Schritt-für-Schritt-Anweisungen kann ich `iFixit.com` nur wärmstens empfehlen. iFixit arbeitet nach der Devise »Kostenlose Reparaturanleitungen, die auch bearbeitbar sind« und wird von Technikern wie Ihnen erstellt, die einem Problem begegnen, die einzelnen Schritte zur Lösung dokumentieren und die Einzelheiten online stellen (Abbildung 23.31). Der nächste Techniker, der über das gleiche Problem stolpert, braucht dann das Rad nicht neu zu erfinden. Die Einkünfte, die iFixit aus dem Verkauf von Bauteilen und Werkzeugen erzielt, kommen übrigens der Website zugute.

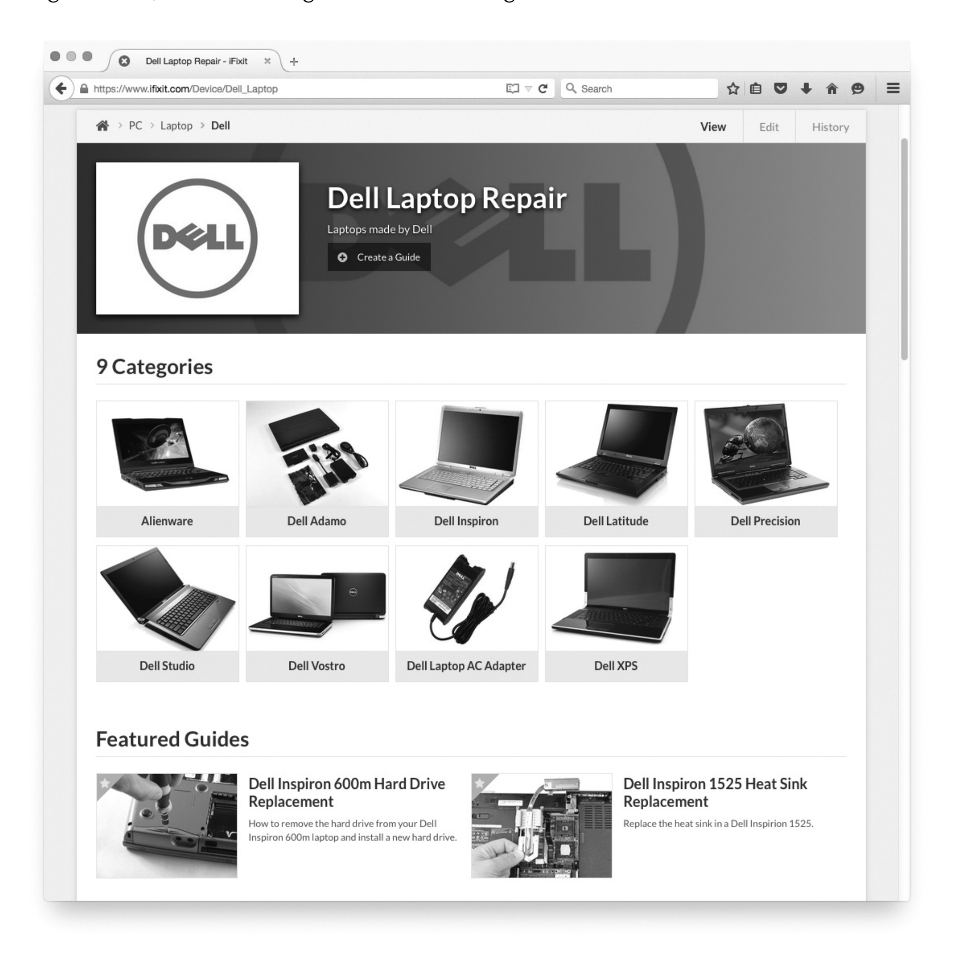


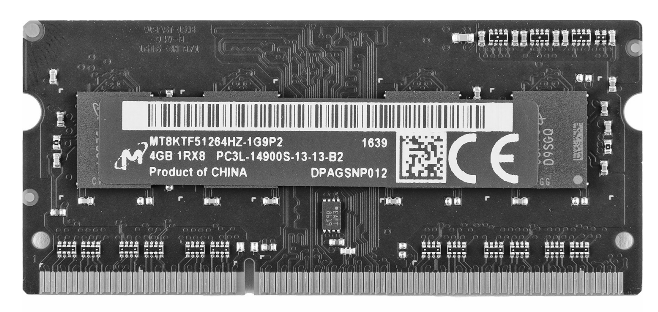
Abb. 23.31: Einige der Schritt-für-Schritt-Anweisungen zur Reparatur eines Dell-Laptops

23.4.2 Typische Aufrüstungen

Jeder Techniker sollte dazu in der Lage sein, die gängigsten modularen Komponenten eines tragbaren Computers aufzurüsten oder auszutauschen, nämlich RAM und Festplatte bzw. SSD.

RAM

Tragbare Computer von der Stange sind typischerweise nur sehr bescheiden mit Arbeitsspeicher ausgestattet, sodass Laptopbesitzer diesen häufig recht schnell aufrüsten (lassen). Glücklicherweise besitzen die meisten Laptops Steckplätze zur Erweiterung des Arbeitsspeichers. Ältere Geräte verwenden DDR- oder DDR2-SO-DIMMs mit 200 Pins und aktuelle Systeme DDR3-SO-DIMMs mit 204 Pins (Abbildung 23.32) oder DDR4-S0-DIMMs mit 260 Pins. Lesen Sie in Kapitel 4 nach, um Ihre Kenntnisse über RAM-Technologien aufzufrischen, aber denken Sie daran, dass sich die Anzahl der Pins von RAM-Bausteinen für Desktops und Laptops möglicherweise unterscheiden, auch wenn die Spezifikation ansonsten übereinstimmt.



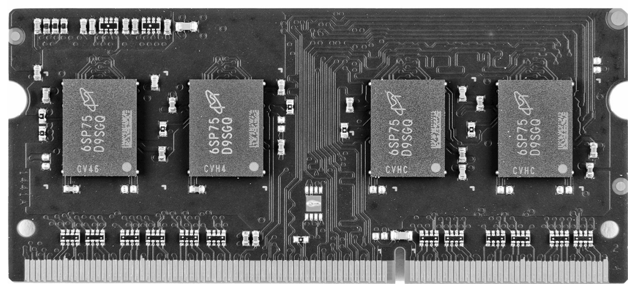


Abb. 23.32: SO-DIMM mit 204 Pins (Vorder- und Rückseite)

Wichtig

Rechnen Sie in der Prüfung mit Fragen zur Installation und Konfiguration des Arbeitsspeichers von Laptops. Typischerweise verwendet ein Benutzer Programme, die mehr Arbeitsspeicher als vorhanden benötigen, sodass der Computer ständig auf die Auslagerungsdatei zugreift, was zu einer erbärmlichen Geschwindigkeit führt. Der Austausch der RAM-Bausteine gegen größere oder das Hinzufügen von Arbeitsspeicher wird die Leistung drastisch verbessern.

RAM aufrüsten oder austauschen Die RAM-Erweiterung erfolgt bei tragbaren Computern in mehreren Schritten. Erst müssen Sie natürlich die richtigen Speichermodule besorgen. Sehen Sie dazu auf der Website des Herstellers oder im Handbuch (falls vorhanden) des tragbaren Computers nach und informieren Sie sich über den benötigten RAM-Typ. Nachdem Sie das wissen, müssen Sie die aktuelle RAM-Konfiguration des Systems herausfinden. Wenn Sie das System von 4 auf 8 GB aufrüsten möchten, müssen Sie wissen, ob ein 4-GB-Modul oder zwei 2-GB-Module darin verbaut sind.

Außerdem stellt jeder tragbare Computer einen Techniker bei Speichererweiterungen vor neue Herausforderungen, weil sich die RAM-Bausteine stets an anderer Stelle befinden. Meistens müssen Sie eine Abdeckplatte an der Unterseite entfernen (Abbildung 23.33) und den RAM-Baustein nach Wegdrücken der Halterungsfedern herausnehmen (Abbildung 23.34). Entnehmen Sie den alten Baustein vorsichtig und setzen Sie den neuen ein, indem Sie die Schritte in umgekehrter Reihenfolge durchführen.

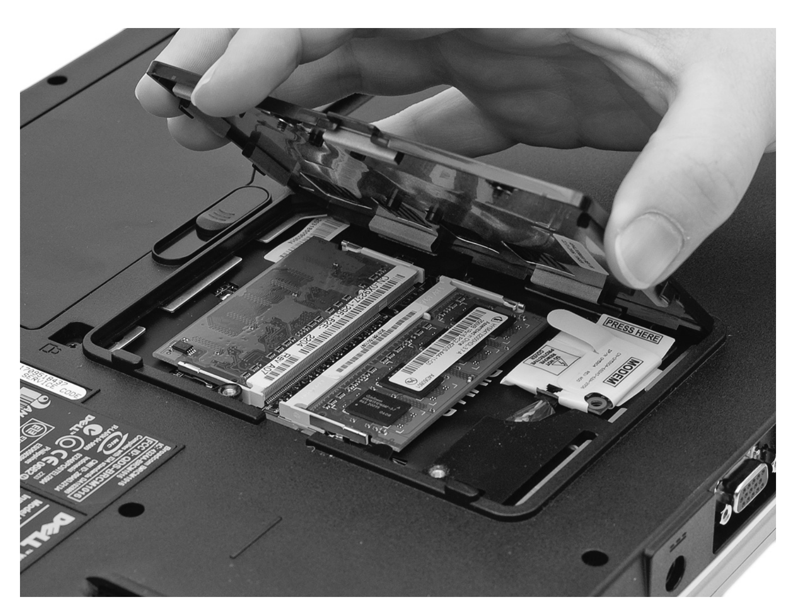


Abb. 23.33: Öffnen der Abdeckplatte



Abb. 23.34: Entnahme des Speichermoduls

Denken Sie daran, das Notebook vor dem Ein- oder Ausbau des Arbeitsspeichers von allen Spannungsquellen zu trennen. Nehmen Sie, falls möglich, den Akku heraus und trennen Sie das Netzteil vom Stromnetz. Wird dies übersehen, kann es zu einer Beschädigung des Geräts kommen. Falls der Akku nicht entnehmbar ist, sollten Sie sich beim Hersteller darüber informieren, ob es ungefährlich ist, am Gerät zu arbeiten, oder weitere Vorsichtsmaßnahmen zu treffen sind.

Vorsicht

Manche Geräte besitzen sowohl fest verbaute als auch entnehmbare Akkus.

Gemeinsam genutzter Speicher Einige Laptops (und Desktops) unterstützen gemeinsam genutzten Speicher (*Shared Memory*). Die Grafikkarte selbst besitzt aus Kostengründen weniger Arbeitsspeicher und nutzt stattdessen den Arbeitsspeicher des Systems.

Der offensichtliche Vorteil des gemeinsam genutzten Speichers liegt in der preiswerteren Grafikkarte (und dem preiswerteren Laptop!), die aber dennoch ähnlich leistungsfähig wie die mit viel mehr Speicher ausgestattete Alternative ist. Der Nachteil besteht darin, dass die Leistung des Gesamtsystems mehr oder weniger stark beeinträchtigt wird, da ja nun Teile des System-RAMs Programmen nicht mehr zur Verfügung stehen. (Es ist ein wenig irreführend, wenn man von *gemeinsamer* Nutzung spricht, da die Grafikkarte einen Teil des RAMs für sich nutzt. Diese Teile des System-RAMs werden *nicht* sowohl vom Grafikprozessor und der CPU genutzt.)

Bei einigen Systemen können Sie festlegen, wie viel Speicher für die Grafikkarte als Shared Memory zur Verfügung gestellt werden darf, während Sie diese Funktion bei anderen nur aktivieren oder deaktivieren können. Die Einstellungen befinden sich im CMOS-Setup jener Systeme, die Shared Memory unterstützen.

Wenn Sie bei einem Laptop mit Shared Memory den Arbeitsspeicher des Systems erweitern, führt dies zu einer Leistungssteigerung. Auch wenn dann die Grafikleistung scheinbar besser wird, ist das nicht wirklich so. Es wird vielmehr die Gesamtleistung des Systems verbessert, weil dem Betriebssystem und der CPU mehr Arbeitsspeicher zur Verfügung stehen. Auf einigen Laptops kann sich auch die Grafikleistung verbessern, aber das ist von den CMOS-Einstellungen abhängig. Wenn für den gemeinsam genutzten Speicher vorher nicht die Maximalwerte verwendet wurden, dann wird das System durch eine Speichererweiterung schneller und die Grafikleistung steigt ebenfalls, wenn man dabei auch die Größe des gemeinsam genutzten Speichers heraufsetzen kann.

Festplatte/SSD

Der Austausch einer Festplatte, einer SSD oder eines Hybridlaufwerks (SSHD) eines tragbaren Computers ist relativ einfach, besonders wenn das Gerät nicht älter als ein paar Jahre ist. 2,5-Zoll-SATA-Laufwerke sind heute der Standard in allen modernen Laptops. Obwohl sie deutlich kleiner als normale 3,5-Zoll-Laufwerke sind, bieten sie dieselben Funktionen und Konfigurationsmöglichkeiten.

Die kleinformatigeren Festplatten verfügen allerdings erwartungsgemäß über relativ kleinere Speicherkapazitäten als ihre 3,5-Zoll-Verwandten. 2,5-Zoll-Festplatten sind heute mit Kapazitäten bis zu 5 TB erhältlich, während 3,5-Zoll-Festplatten teilweise bereits mehr als 8 TB an Daten aufnehmen können! Leider bieten die meisten Laptops nur Platz für Laufwerke, die 7 oder 9,5 Millimeter dick sind, die größten 2,5-Zoll-Laufwerke sind jedoch 15 Millimeter dick. Die größten 2,5-Zoll-Laufwerke, die in einen typischen Laptop passen, besitzen eine Kapazität von 2 TB.

Wichtig

Es gibt auch 1,8-Zoll-Laufwerke, die aber kaum noch eine Rolle spielen, da sie in MP3-Playern und anderen tragbaren Geräten weitgehend durch Flash-Speicher ersetzt wurden. Wenn Ihnen ein solches Laufwerk über den Weg läuft, dürfte es sich höchstwahrscheinlich um einen einfachen älteren MP3-Player handeln.

Bei älteren Laptops, die noch PATA-Laufwerke verwenden, müssen Sie möglicherweise das Laufwerk speziell konfigurieren (Master, Slave oder Cable Select). Informieren Sie sich daher beim Hersteller (oder zumindest im Handbuch) stets nach möglichen Besonderheiten. Ansonsten gibt es zwischen den 2,5- und den 3,5-Zoll-Laufwerken keine nennenswerten Unterschiede (Abbildung 23.35).



Abb. 23.35: 2,5- und 3,5-Zoll-Laufwerke sind weitgehend identisch.

Hinweis

Falls Sie einen neueren Laptop besitzen, stehen die Chancen nicht schlecht, dass er einen der kleineren SSD-Formfaktoren verwendet, nämlich mSATA oder M.2. Sie wurden in Kapitel 8 schon erläutert. Lesen Sie bei Bedarf dort nach, um Ihre Kenntnisse aufzufrischen.

Die meisten Hersteller machen es ziemlich einfach, ein mSATA- oder M.2-Laufwerk nachzurüsten. Entfernen Sie die Bodenplatte oder die Abdeckung des Laufwerks. Lösen Sie die winzigen Halteschrauben und entnehmen Sie das alte Laufwerk. Platzieren Sie das neue Laufwerk an Ort und Stelle und befestigen Sie es mit den Halteschrauben. Das war schon alles, zumindest was die Hardware betrifft.

Eine herkömmliche Festplatte durch eine SSD zu ersetzen ist eine wirklich empfehlenswerte Aufrüstung. Sie bekommen zwar für das gleiche Geld deutlich weniger Speicherkapazität, aber dieser Kompromiss kann es wert sein, denn erstens benötigt eine SSD sehr viel weniger Energie als eine herkömmliche Festplatte (wodurch die Akkulaufzeit verlängert wird), und zweitens ist jede SSD um Größenordnungen schneller als eine Festplatte, sodass die Gesamtleistung des Systems steigt. Für einen gewissen Zeitraum stellten SSHDs (Hybridlaufwerke) einen guten Kompromiss zwischen der Geschwindigkeit einer SSD und der Speicherkapazität herkömmlicher Festplatten dar. Zwischenzeitlich sind die Preise für SSDs gesunken und die Speicherkapazitäten gewachsen, daher erscheinen SSHDs zunehmend als keine gute Wahl. SSDs mit einer Kapazität von 2 bis 4 TB sind bereits verfügbar, aber immer noch ziemlich teuer. 500-GB-SSDs sind schon für rund 50 Euro erhältlich.

Tipp: Vergleich von HDDs und SSDs

Derzeit bekommt man bei einer HDD für denselben Preis etwa die doppelte Speicherkapazität einer SSD. Sie können zum Preis von ca. 50 Euro eine 500-GB-SSD oder eine 2,5-Zoll-HDD mit 1 TB Speicherkapazität kaufen. Stellen Sie Preisvergleiche an. Lohnt es sich für Sie oder Ihre Kunden, von HDD auf SSD zu wechseln?

Die Vorgehensweise beim Austausch der Festplatte ähnelt derjenigen beim Austausch des Arbeitsspeichers. Die Abdeckplatte des Laufwerks befindet sich meistens an einem der Ränder oder bei einem

Fach auf der Unterseite des tragbaren Computers. Entfernen Sie die Schrauben (Abbildung 23.36), entnehmen Sie dann das alte Laufwerk und setzen Sie das neue vorsichtig ein (Abbildung 23.37). Befestigen Sie die Abdeckung wieder und starten Sie den Rechner. Besorgen Sie sich nun eine Betriebssystem-DVD oder einen startfähigen USB-Stick und bereiten Sie sich auf eine Neuinstallation vor.



Abb. 23.36: Halteschrauben der Abdeckung entfernen



Abb. 23.37: Einsetzen des neuen Laufwerks

23.4.3 Andere Komponenten ersetzen

Wenn Sie etwas anderes als RAM oder Festplatte ersetzen möchten, müssen Sie sich mit den Eigenarten der Laptop-Reparatur auseinandersetzen. Manche Komponenten sind leicht ersetzbar, indem

man sie anhebt, ein Flachbandkabel ablöst und beim Einbau des Ersatzteils in umgekehrter Reihenfolge vorgeht. Bei anderen Bauteilen hingegen kann es hingegen erforderlich sein, den Laptop nahezu vollständig zu zerlegen – solch ein Austausch ist um Größenordnungen schwieriger. Da sich die verschiedenen Laptops so sehr unterscheiden, gibt es in diesem Abschnitt keine schrittweise Anleitung, sondern einen Leitfaden für den Austausch von Komponenten. Sie sollten sich jedoch darüber im Klaren sein, dass bei neueren Systemen, wie vorhin bereits erwähnt, tendenziell mehr integrierte Komponenten verbaut werden. Vergewissern Sie sich also, dass die zu ersetzende Komponente auch tatsächlich austauschbar ist.

Ersetzbare Komponenten

Für das Ersetzen anderer Komponenten als RAM oder Festplatte ist oft mehr Arbeit erforderlich, es ist im Allgemeinen aber durchaus machbar. Unter »ersetzbare Komponenten« verstehe ich hier Akku, Tastatur, optisches Laufwerk, interne Lautsprecher, Einbaurahmen, Erweiterungskarten und CPU.

Akku Wenn die Leistung des Akkus nicht mehr zumutbar ist, können Sie ihn durch ein Modell des Herstellers oder eines aus dem Zubehörhandel ersetzen. Normalerweise ist der Akkutausch ein simpler Vorgang, jedenfalls sofern er nicht fest verbaut ist, aber gelegentlich ist gar nicht der Akku die Ursache des Problems, sondern eine unpassende oder defekte Ladeelektronik. Es kann daher sein, dass ein neuer Akku keine Verbesserung bringt. Hier hilft nur Ausprobieren.

Tastatur Zum Entfernen der Tastatur ist oftmals ein kleiner Spatel erforderlich, um diese vorsichtig herauszuhebeln. Halten Sie aber auch nach Schrauben, Klammern usw. Ausschau! Die Tastatur ist mit einem kurzen, äußerst empfindlichen, folienartigen Flachbandkabel angeschlossen, das oft durch Klebeband fixiert ist. Das Ersetzen ist zwar ziemlich »fummelig«, aber machbar.

Optisches Laufwerk Das Ersetzen eines optischen Laufwerks kann eine echte Herausforderung sein. Bei modular aufgebauten Systemen muss es nur entnommen und ersetzt werden. Ist das Laufwerk aber Bestandteil des internen Einbaurahmens, steht Ihnen eine komplette Zerlegung des Geräts bevor. (Im Abschnitt *Integrierte Bauteile* finden Sie Tipps zur Demontage eines tragbaren Computers.)

Lautsprecher Das Ersetzen der Lautsprecher ist entweder sehr einfach oder aber eine echte Qual, je nachdem, wie die Lautsprecher im Gehäuse verbaut sind. Bei manchen Geräten sind die Lautsprecher außerhalb des internen Einbaurahmens montiert. Öffnen Sie das Gehäuse, ziehen Sie die Lautsprecher heraus und lösen Sie die Kabel. Der Einbau erfolgt wieder in umgekehrter Reihenfolge. Sind die Lautsprecher aber in den internen Einbaurahmen integriert, müssen Sie den tragbaren Computer komplett demontieren, um an die Lautsprecher heranzukommen (siehe Abschnitt *Integrierte Bauteile*).

Einbaurahmen Die ausgeklügelte Elektronik, die das Funktionieren des Laptops erst ermöglicht, wird durch verschiedene Bauteile aus Kunststoff, Metall oder Gummi zusammengehalten, die verloren oder kaputtgehen können. Im Allgemeinen sind sie zwar ziemlich stabil, aber im Laufe der Zeit (oder bei einem Unfall) können sie sich verziehen, verbiegen, zerbrechen oder auf andere Weise unbrauchbar werden. Diese Bauteile sind ebenfalls ersetzbar, vorausgesetzt, dass sie passender Ersatzteile habhaft werden können.

Dazu benötigen Sie die exakte Bezeichnung des Modells und eventuell auch die Teilenummer des Herstellers. Viele Bauteile sind einander sehr ähnlich und manche kommen in vielen anderen Laptops ebenfalls zum Einsatz. Unter Umständen ist ein benötigtes Ersatzteil nur als Bestandteil einer kompletten Baugruppe erhältlich. Sie müssen dann wohl oder übel einen lächerlich hohen Preis für die erforderliche Komponente bezahlen.

Erweiterungskarten Viele tragbare Computer können Erweiterungskarten aufnehmen. Bei modular konzipierten Modellen gibt es dann wie beim RAM ebenfalls eine Abdeckung auf der Unterseite des Computers, die Ihnen Zugang zu den Steckplätzen gewährt. Sie können auf diese Weise beispielsweise eine 802.11n-Karte durch eine 802.11ac-Karte ersetzen, um die WLAN-Fähigkeiten eines Gerätes deutlich zu verbessern. Oder Sie können das Bluetooth-Modul durch eine verbesserte Version ersetzen. Abbildung 23.38 zeigt einen geöffneten Laptop mit einem Mini-PCIe-Steckplatz.



Abb. 23.38: Geöffneter Laptop mit Erweiterungssteckplatz

Hinweis

Fragen Sie beim Hersteller nach, ob es eine WLAN-Erweiterungskarte gibt, die mit dem fraglichen Modell kompatibel ist. Wenn eine Karte in den Steckplatz passt, heißt das noch lange nicht, dass sie auch funktioniert.

Wie auch bei der Installation von RAM-Bausteinen müssen Sie elektrostatische Entladungen vermeiden und das Gerät von allen Spannungsquellen trennen. Falls Akku oder Netzteil nicht entfernt werden, kann es zu Kurzschlüssen auf dem Mainboard kommen, und das wünscht sich nun wirklich niemand.

Es gibt noch einen weiteren Punkt zu bedenken und dieser bezieht sich auf drahtlose Netzwerkkarten. Sie müssen nicht nur die Karte ordnungsgemäß anschließen, sondern auch das Antennenkabel wieder anstecken und nicht selten auch eine separate Stromversorgung. Geben Sie beim Entfernen der alten Karte daher unbedingt auf diese wichtigen Verbindungskabel acht.

Man findet zwei verschiedene Erweiterungssteckplätze in tragbaren Computern: Mini-PCIe und M.2. Ältere Geräte (vor 2013) verwenden Mini-PCIe, während sich bei neueren Modellen schnell M.2 durchgesetzt hat.

CPU Das Ersetzen der CPU eines modernen tragbaren Computers bereitet im Vergleich zum Ersatz von Arbeitsspeicher oder einer Mini-PCIe-Erweiterungskarte eine Menge Arbeit, folgt aber denselben Regeln. Viele CPUs sind auf der Unterseite des Mainboards montiert, sodass die Wärme vornehmlich nach unten abgegeben wird. Wenn das Gerät ordentlich auf einer flachen Oberfläche steht, wird die warme Abluft nach hinten abgeführt, nicht in Richtung des Benutzers. Bei Systemen dieser Art greifen Sie auch von der Unterseite des Rechners aus auf die CPU zu.

Wie Sie in Abbildung 23.39 sehen können, besitzt die CPU eine aufwendige Kühlkörper-Lüfter-Kombination, auf der neben der CPU auch der Chipsatz integriert ist. Das Bauteil wird an mehreren Stellen festgeschraubt und der Kühler besitzt eine eigene Stromversorgungsleitung. Abgesehen von der Größe der Schrauben gibt es beim Ersetzen einer Mobil-CPU keinen Unterschied zum Ersetzen einer Desktop-CPU, wie Sie es aus Kapitel 3, *Mikroprozessoren*, bereits kennen.

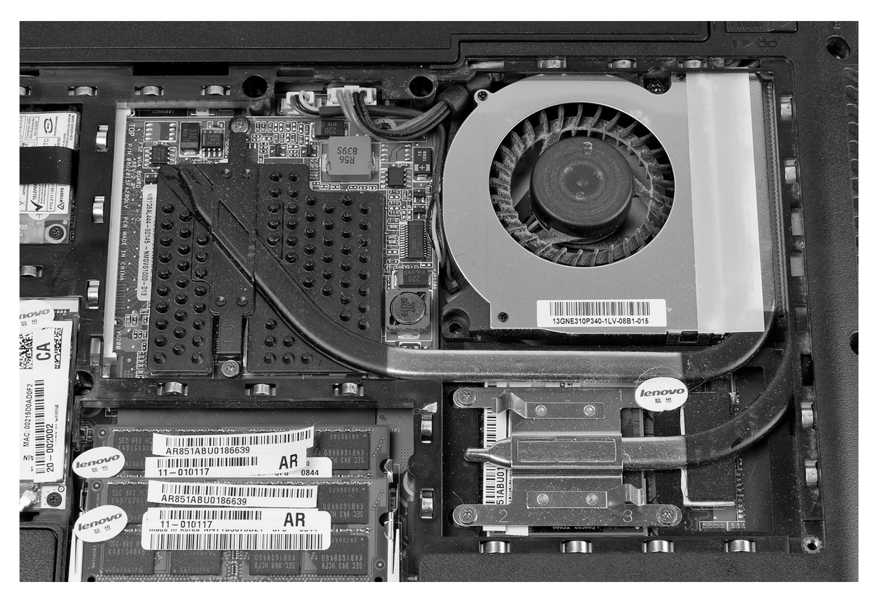


Abb. 23.39: CPU-Kühlkörper und Lüfter

Trennen Sie das Notebook zunächst von sämtlichen Spannungsquellen und entfernen Sie auch den Akku oder treffen Sie die vom Hersteller empfohlenen Vorsichtsmaßnahmen, wenn der Akku fest verbaut ist. Entfernen Sie nun die Abdeckplatte der CPU und dann die Kühlkörper-Lüfter-Kombination. Entnehmen Sie die CPU, setzen Sie eine neue ein, tragen Sie etwas Wärmeleitpaste auf und befestigen Sie den Kühlkörper wieder. Vergessen Sie nicht, den Lüfter wieder an die Stromversorgung anzuschließen. Und schon sind Sie fertig.

Einige ältere Laptops verwenden eine passive Kühlung. Hier sitzt die CPU daher auf der Oberseite des Mainboards. Der Kühlkörper befindet sich unter der Tastatur, sodass Sie bei derartigen Systemen erst die Tastatur und dann den Kühlkörper entfernen müssen, um die CPU freizulegen.

Display und zugehörige Komponenten

Das Ersetzen eines Laptop-Displays stellt eine besondere Herausforderung dar. Es besteht aus Bauteilen, die man erwartet, wie Panel, Hintergrundbeleuchtung und Inverter (bei älteren Geräten), es gibt jedoch weitere Komponenten, wie WLAN-Antenne, Webcam und Mikrofon. Noch schwieriger wird es bei Touchscreen-Displays. Die CompTIA erwartet von Ihnen, dass Sie wissen, wie ein Display und die zugehörigen Komponenten ersetzt (bzw. installiert) werden.

Wichtig

In den Anfang 2019 erschienenen Lernzielen der CompTIA A+-Prüfung 1001 ist von LCD- und OLED-Displays für Laptops die Rede. Wie Sie aus Kapitel 17 wissen, gibt es Laptops mit OLED-Display so gut wie gar nicht (zumindest nicht für Endkunden). Das Ersetzen eines OLED-Displays erfolgt aber praktisch auf die gleiche Art und Weise wie das eines LCD-Displays.

Das Ersetzen des Bildschirms (Flachbildschirm, Touchscreen, Digitizer), des Inverters, der WLAN-Antenne oder des Mikrofons erfolgt durch die gleichen Schritte. Entfernen Sie den Kunststoffrahmen, am besten mit einem Spatel oder einem anderen Werkzeug des iFixit-Sets und lösen Sie die gegebenenfalls freigelegten Schrauben. Entnehmen Sie den Bildschirm, nachdem Sie möglicherweise vorhandene intern angeschlossene Bauteile gelöst und entfernt haben. Genauer kann ich das nicht beschreiben, weil sich alle Modelle voneinander unterscheiden, aber meistens sind die Komponenten mit kleinen Schrau-

ben oder Klammern befestigt oder angeklebt. Dann müssen Se möglicherweise vorhandene Datenkabel trennen. Wenn Sie nur Webcam oder Mikrofon ersetzen, müssen Sie die anderen Bauteile (höchstwahrscheinlich) nicht abtrennen, aber wenn Sie den Bildschirm oder den Inverter austauschen, müssen Sie alles entfernen.

Machen Sie Fotos mit Ihrem Smartphone und achten Sie darauf, wie die Stecker verbunden sind. Gehen Sie nicht hastig vor, wenn Sie es mit so vielen kleinen Steckern und Bauteilen zu tun haben. Notieren Sie sich, wo die Schrauben verschiedenen Typs hingehören. Diese zusätzliche Arbeit wird durch einen erfolgreich reparierter Laptop belohnt. Glauben Sie mir!

Wichtig

Rechnen Sie damit, dass in der Prüfung Fragen zum Ersetzen des Bildschirms oder anderer zugehöriger Komponenten eines Laptops vorkommen. Diese Fälle sind eindeutig: zerbrochener Bildschirm, nicht reagierender Touchscreen, kein WLAN-Empfang wegen defekter Antenne und so weiter.

Integrierte Bauteile

Beim Ersetzen mancher Komponenten müssen Sie beim Laptop ernsthaft Hand anlegen, viele hochempfindliche Bauteile entfernen und es so weit auseinandernehmen, bis der interne Einbaurahmen freiliegt. Ich überlasse solche Reparaturen den Spezialisten, weil diese über die Spezialwerkzeuge und die Erfahrung verfügen, um derartige Aufgaben zu erledigen. Die CompTIA erwartet von Ihnen allerdings, dass Ihnen der Vorgang an sich bekannt ist, daher werde ich ihn kurz skizzieren. Hier sind drei Komponenten betroffen: Gleichstrom-Anschlüsse, Touchpad und Mainboard.

Wichtig

Es könnte sein, dass in der Prüfung eine Frage zum Austausch der Grafikkarte eines Laptops gestellt wird, in der Praxis kommt das aber sehr selten vor. In den letzten Jahren gab es nur eine Handvoll Modelle mit austauschbarer Grafikkarte. In den meisten Fällen ist sie fester Bestandteil des Mainboards. Ist die Grafikkarte defekt, muss das Mainboard ausgetauscht werden.

Je nach Hersteller lassen sich tragbare Computer auf zweierlei Weise öffnen. Entweder müssen Sie sich nach dem Entfernen der Tastatur Schicht um Schicht von oben nach unten vorarbeiten oder aber nach Entfernen der Bodenplatte von unten nach oben. Auf die Einzelheiten wie die Verbindungen der Einzelteile und deren Position müssen Sie bei beiden Vorgehensweisen achtgeben. Am besten legen Sie sich ein System zurecht, um die mehrere Dutzend Schrauben zu sortieren.

Bei allen beschriebenen Ersetzungen muss der Bildschirm vom Gehäuse des tragbaren Computers abgetrennt werden. Neben dem Auffinden der Verbindungspunkte und dem Entfernen der richtigen Schrauben müssen Sie auch auf die Kabel zur Ansteuerung des Bildschirms und auf das Verbindungskabel zur im Bildschirmrahmen befindlichen Antenne achtgeben.

Sobald Sie das Gerät zerlegt haben, können Sie die betreffende Komponente ersetzen und damit beginnen, Stück für Stück wieder eine zusammenhängende Einheit aus all den herumliegenden Einzelteilen zusammenzubauen. Lassen Sie beim Wiederherstellen der Kabelverbindungen unbedingt absolute Akribie walten! Es gibt für einen Techniker kaum eine schlimmere Erfahrung, als beim Austausch eines Touchpads nach stundenlanger Schrauberei feststellen zu müssen, dass irgendeine Verbindung nicht funktioniert und alles von vorne losgeht.

Wichtig

Wenn Sie den Gleichstrom-Anschluss auf dem Mainboard ersetzen müssen, beansprucht das besondere Aufmerksamkeit. Da dieses Bauteil fest verlötet ist, müssen Sie nicht nur den tragbaren Computer komplett zerlegen, sondern auch das alte Bauteil entlöten und das neue einlöten. Dann müssen Sie alles wieder

zusammenbauen und darauf hoffen, dass es funktioniert. Die CompTIA kann von A+-Technikern keinesfalls erwarten, dass sie wissen, *wie* eine solche Aufgabe erledigt wird, aber sehr wohl, dass sie wissen, *ob* sie erledigt werden kann. Im Übrigen dürfen Sie mir glauben, dass spezialisierte Techniker *jede* Komponente eines tragbaren Computers ersetzen können – auch den Gleichstrom-Anschluss.

23.5 Fehlerbehebung bei tragbaren Computern

Viele der für Desktop-Systeme geeigneten Techniken der Fehlersuche lassen sich auch auf Laptops anwenden. Wenn Sie einen Laptop zerlegen, dann sollten Sie dabei z.B. ebenfalls auf die entsprechenden Vorkehrungen achten. Verwenden Sie geeignetes Werkzeug, dokumentieren Sie Ihre Schritte, beschriften Sie die Teile und bewahren Sie diese ordentlich auf, damit Sie alle Teile und Schrauben auch wiederfinden. Außerdem gibt es einige spezielle Verfahrensweisen für Laptops, die Sie ausprobieren sollten.

23.5.1 Stromversorgung und beeinträchtigte Leistung

Die meisten Probleme mit Laptops haben damit zu tun, wie gut (oder schlecht!) sie funktionieren. Betrachten wir also einige der typischen Probleme, die mit Stromversorgung, Leistung und Wärme zu tun haben.

Der Laptop lässt sich nicht einschalten

- Überprüfen Sie die Stromversorgung, indem Sie ein anderes elektrisches Gerät an die Steckdose anschließen. Wird das andere Gerät mit Strom versorgt, ist die Steckdose in Ordnung.
- Wenn die Steckdose in Ordnung ist, schließen Sie den Laptop daran an und versuchen Sie, ihn einzuschalten. Wenn keine LEDs leuchten, ist möglicherweise das Netzteil defekt. Tauschen Sie es gegen ein Netzteil aus, von dem Sie wissen, dass es funktioniert.
- Auch ein defektes Peripheriegerät kann dafür sorgen, dass sich der Laptop nicht einschalten lässt. Entfernen Sie alle Peripheriegeräte, wie beispielsweise USB-, FireWire- oder Thunderbolt-Geräte.

Beeinträchtigte Leistung

- Der häufigste Grund für eine beeinträchtigte Leistung sind Anwendungen und Prozesse, die sehr viele Ressourcen in Anspruch nehmen. Alle Betriebssysteme bringen Werkzeuge mit, um das zu überprüfen. Verwenden Sie unter Windows den Task-Manager oder in macOS die Aktivitätsanzeige, um solchen Problemen auf den Grund zu gehen. Möglicherweise muss eine Anwendung sofort beendet werden oder Sie müssen einen Neustart durchführen. Vielleicht ist es auch erforderlich, die fragliche Anwendung zu aktualisieren.
- Im Extremfall scheint das System zum völligen Stillstand gekommen zu sein. Falls das Problem nicht von selbst verschwindet und das System nicht mehr reagiert, müssen Sie womöglich einen »harten« Reset ausführen, wodurch es zum Verlust ungesicherter Änderungen kommen kann. Normalerweise reicht es, die Einschalttaste zehn Sekunden lang gedrückt zu halten, aber konsultieren Sie im Zweifelsfall die Website des Herstellers oder das Handbuch, um die richtige Vorgehensweise zu ermitteln. Wenn der Akku entnehmbar ist, können Sie das Gerät möglicherweise auch neu starten, indem Sie den Akku entfernen, wieder einsetzen und das Gerät einschalten.

Hinweis

Sowohl der Hersteller als auch Dritte sprechen manchmal von einem »harten« und einem »weichen« Reset. Sie sollten wissen, dass es sich hierbei nicht um dasselbe wie einen Kaltstart bzw. Warmstart handelt, insbesondere dann, wenn Sie es mit Hybridgeräten zu tun haben. Halten Sie sich also an die Anweisungen des Herstellers und vergewissern Sie sich, dass Sie korrekt vorgehen. Mehr zum Thema Kalt- und Warmstart finden Sie in Kapitel 25.

Probleme mit dem Akku

- Ein aufgequollener oder geplatzter Akku wird vermutlich zunächst gar nicht bemerkt, und die damit einhergehenden Symptome sind schwer erkennbar, wenn man nicht damit rechnet. Die Ursache dafür ist zumeist eine Überladung des Akkus durch eine fehlerhafte Ladeelektronik, die das eigentlich verhindern soll. Die ersten auftretenden Symptome sind, dass der Laptop nicht völlig plan auf einer glatten Oberfläche steht, der zugeklappte Bildschirm nicht mehr exakt mit dem Rand des Gehäuses abschließt, Probleme mit Eingabegeräten wie Touchpad oder Tastatur und Schwierigkeiten beim Einlegen bzw. Entfernen des Akkus. Früher oder später kann dann das Gehäuse des Geräts ganz offensichtlich verformt sein. Das Akkugehäuse selbst ist für ein geringfügiges Aufquellen des Akkus ausgelegt, allerdings steigt in diesem Fall die Gefahr, dass der Akku durchbohrt oder durchstochen wird – und das kann wirklich gefährlich sein. Ignorieren Sie solche Hinweise nicht. Entnehmen Sie den Akku vorsichtig und überprüfen Sie ihn. Falls Sie einen Defekt feststellen, sollten Sie ihn sicher verpackt zu einer geeigneten Entsorgungsstelle bringen.
- Wenn der Akku eines Laptops nicht richtig aufgeladen wird, kann dies zwei Ursachen haben. Einerseits kann der Akku, andererseits die Ladeelektronik bzw. das Netzteil defekt sein. Verwenden Sie einen Akku, von dem Sie wissen, dass er in Ordnung ist. Wenn der Laptop dann funktioniert, haben Sie den Schuldigen gefunden; ersetzen Sie den Akku. Alternativ können Sie auch den Akku entfernen und den Laptop nur am Netzteil betreiben. Wenn das funktioniert, dann wissen Sie, dass das Netzteil in Ordnung ist. Falls nicht, ersetzen Sie das Netzteil.
- Der Grund für die geringe Laufzeit eines ordnungsgemäß ladenden Akkus ist normalerweise harmlos. Für gewöhnlich hat er hinreichend viele Ladezyklen erlebt, ist damit am Ende seiner Lebensdauer angekommen und muss ersetzt werden. Es könnte allerdings auch sein, dass irgendein Programm oder irgendein Gerät besonders viel Strom verbraucht. Überprüfen Sie dann, ob irgendeins der sonst deaktivierten drahtlosen Geräte eingeschaltet ist. Folgen Sie den im vorhergehenden Abschnitt genannten Ratschlägen, wenn Programme Schwierigkeiten verursachen.

Überhitzung

- Da Überhitzung sowohl Ursache als auch Symptom verschiedener Probleme sein kann, sollten Sie darauf achten, ob Geräte sich beim Anfassen sehr warm oder wärmer als sonst anfühlen. Prüfen Sie, welche Teile des Gehäuses besonders warm sind, denn das kann ein wichtiger Hinweis auf die Ursache sein. Wenn sich ein Gerät gefährlich heiß anfühlt, sollten Sie es sicherheitshalber lieber abschalten, anstatt den Grund der Überhitzung herauszufinden. Fahren Sie das System herunter, entnehmen Sie den Akku (sofern möglich) und platzieren Sie das Gerät auf einer kühlen, harten Oberfläche ohne direkte Sonneneinstrahlung und sorgen Sie dafür, dass die heißesten Teile möglichst an der Luft abkühlen können.
- Halten Sie nach Hinweisen auf eine Überhitzung Ausschau, wie spontane Neustarts, Grafikfehler oder Pieptöne des internen Lautsprechers und überprüfen Sie, dass eine Überhitzung als mögliche Ursache auszuschließen ist.
- Achten Sie auf Lüftergeräusche. Manche tragbaren Computer besitzen keine Lüfter, aber völlige Stille kann auf einen defekten Lüfter hindeuten, und ungewöhnliche Geräusche könnten ein Anzeichen dafür sein, dass der Lüfter gerade seinen Geist aufgibt.
- Sie sollten außerdem wissen, unter welchen Umständen mit einem heißen Gerät zu rechnen ist. Stark belastete oder ladende Geräte erzeugen eine Menge Wärme. Folgen Sie den in den beiden vorhergehenden Abschnitten genannten Ratschlägen, um herauszufinden, ob Komponenten aktiv sind, die eigentlich deaktiviert sein sollten, sich aber dennoch warm anfühlen und um verrücktspielende Programme zu beenden. Trennen Sie das Gerät von der Stromversorgung, wenn es aufgeladen wird, und beobachten Sie, ob es dann abkühlt. Falls Sie nichts Außergewöhnliches entdecken können, das Gerät aber trotzdem heißläuft, liegt vermutlich ein Problem mit der Luftzirkulation vor. Überprüfen Sie, ob vielleicht Lüftungsschlitze blockiert sind, und öffnen Sie das Gerät, falls nötig, um Lüfter und Kühlkörper zu kontrollieren.

- Wenn das gesamte Gerät ungewöhnlich warm ist, war es vielleicht direkter Sonneneinstrahlung oder einer sehr warmen Umgebung ausgesetzt. Lassen Sie es abkühlen und prüfen Sie, ob die Probleme verschwinden.

23.5.2 Weitere Komponenten

Verschiedene andere Komponenten können ebenfalls Schwierigkeiten verursachen. Dazu zählen etwa Bildschirm, drahtlose Netzwerkkarten, Audio-Hardware und Eingabegeräte.

Der Bildschirm funktioniert nicht richtig

- Wenn der Laptop bootet (Sie hören Piepser und Laufwerkgeräusche), prüfen Sie zunächst, ob der Bildschirm eingeschaltet ist. Drücken Sie die Tastenkombination zur Aktivierung des Bildschirms, bis er etwas anzeigt. Wenn das nicht hilft, überprüfen Sie den Mikroschalter des LCD-Panels (der kleine Knopf, der sich oft in der Nähe des Bildschirmscharniers befindet und beim Zuklappen des Laptops betätigt wird). Stellen Sie fest, ob dieser Schalter klemmt und den Bildschirm deaktiviert. Wenn es sich um ein Convertible mit abnehmbarem Bildschirm handelt, sollten Sie prüfen, ob er korrekt angesteckt ist und mit Spannung versorgt wird.
- Wenn die Laptop-Anzeige sehr dunkel ist, ist möglicherweise ein Inverter defekt. Der Hinweis besteht hier darin, dass Inverter nie lautlos sterben. Sie können hässlich brummen und geben ein unangenehmes Geräusch von sich, wenn sie endgültig ihren Geist aufgeben. Häufig fallen Inverter in dem Moment aus, wenn Sie das Netzteil des Laptops anschließen, weil sie direkt über das Netzteil mit Strom versorgt werden. Möglicherweise ist auch die Hintergrundbeleuchtung des LCD-Panels ausgefallen, was allerdings vergleichsweise selten geschieht.
- Wenn sich der Bildschirm nicht einschaltet oder Sprünge aufweist, dann können Sie an die meisten Laptops einen externen Bildschirm anschließen, über den Sie sich beim System anmelden können.
- Wenn Sie einen externen Monitor an einem Laptop anschließen, dieser aber kein Bild zeigt, denken Sie daran, dass sowohl die Hardware als auch das Betriebssystem verhindern kann, dass die Anzeige funktioniert. Meist müssen Sie neben der Taste FN eine weitere Taste drücken, um zwischen den verschiedenen Anzeigemodi umzuschalten. Darüber hinaus können Sie diese Einstellung in der Systemsteuerung im Applet ANZEIGE vornehmen oder die Einstellungs-App verwenden.
- Viele Hersteller setzen nun LEDs für die Hintergrundbeleuchtung ein, was zu einem Problem führt, von dem die meisten Techniker dachten, dass es längst erledigt sei: flackernde Bildschirme. Nun ist es so, dass LEDs prinzipiell eigentlich gar nicht flackern können. Bei tragbaren Computern wird allerdings beim Herunterregeln der Bildschirmhelligkeit ein Trick benutzt: Die LEDs werden in schneller Folge ein- und ausgeschaltet, sodass die Pixel beleuchtet bleiben, aber der Bildschirm insgesamt dunkler und gleichzeitig weniger Energie verbraucht wird. Bei manchen Bildschirmen dieser Bauart ist das Flackern nicht nur wahrnehmbar, sondern kann sogar zu Kopfschmerzen und brennenden Augen führen. Bei flackernden LED-Bildschirmen gibt es nur zwei ziemlich radikale Lösungen: Entweder akzeptieren Sie die geringere Akkulaufzeit und regeln die Helligkeit hoch, bis das Flackern verschwindet, oder aber Sie ersetzen das betroffene Gerät.
- Wenn die Bildschirmausrichtung beim Drehen eines tragbaren Windows-Computers nicht angepasst wird, könnte diese Funktion deaktiviert sein. Wenn sie hingegen zum falschen Zeitpunkt angepasst wird, können Sie die automatische Ausrichtung im Applet ANZEIGE deaktivieren. Wenn immer nur eine Ausrichtung verwendet werden soll, können Sie diese dennoch im Applet ANZEIGE und vermutlich auch über eine Tastenkombination ändern.

Drahtlose Geräte funktionieren nicht oder nur sporadisch

- Falls eines der drahtlosen Geräte überhaupt nicht funktioniert, suchen Sie rund um den Laptop nach Schaltern, mit denen die internen drahtlosen Geräte oder der Flugmodus ein- und ausgeschaltet werden.

- Falls bei Ihrem Gerät kürzlich eine Komponente ausgetauscht wurde, bei dem der Bildschirm vom Gehäuse abgetrennt wurde, ist möglicherweise ein nicht angeschlossenes Antennenkabel die Ursache. Bei den meisten Laptops befindet sich die Antenne im Bildschirmrahmen. Überprüfen Sie die Verbindung.
- Probieren Sie es mit der für Ihren Laptop gültigen Tastenkombination (falls vorhanden) zum Einschalten von WLAN-Adapter und Bluetooth.
- Vielleicht befinden Sie sich an der Grenze (falls das WLAN sporadisch funktioniert) oder außerhalb der Reichweite des Netzwerks. Begeben Sie sich mit dem Laptop in die Nähe des Routers oder des Zugriffspunkts, um sich davon zu überzeugen, dass die Probleme nicht nur von einem zu schwachen Signalpegel verursacht werden. Es kann auch zu Problemen führen, wenn zu viele drahtlose Geräte dasselbe Frequenzband verwenden.
- Denken Sie bei Bluetooth-Verbindungen daran, dass beim Koppeln an beiden Geräten eine Konfiguration oder Aktion vorgenommen werden muss. Schalten Sie das Bluetooth-Gerät ein, suchen Sie danach und probieren Sie erneut, die Geräte zu koppeln.
- Falls nur GPS nicht funktioniert, sind möglicherweise die Einstellungen für den Zugriff auf die Ortungsdienste dafür verantwortlich. Überprüfen Sie in der Systemsteuerung in den Applets STANDORTEINSTELLUNGEN und FAMILY SAFETY, ob GPS aktiviert und der Zugriff auf die Ortungsdienste systemweit und für die fragliche Anwendung gestattet ist. Überprüfen Sie in macOS die Systemeinstellungen und in Linux die entsprechende Stelle.
- Falls nur die Nahfeldkommunikation (NFC – Near Field Communication, siehe Kapitel 24) nicht funktioniert, müssen Sie eine Einstellung aktivieren, die es gestattet, mit in der Nähe befindlichen Geräten zu kommunizieren. Öffnen Sie in Windows die PC-Einstellung NETZWERK, um NFC zu aktivieren. (Das funktioniert nur, wenn NFC-Hardware vorhanden ist.)

Probleme mit Audio-Hardware

- Suchen Sie nach mechanischen Schaltern zur Stummschaltung oder Lautstärkeregelung, wenn die Audioausgabe nicht wie erwartet funktioniert, oder sehen Sie im Infobereich der Taskleiste nach, ob die Audioausgabe stumm geschaltet ist. Überprüfen Sie, ob das Ausgabegerät in Ihrem Betriebssystem ordnungsgemäß installiert ist, und vergewissern Sie sich, dass die Anwendung das richtige Ausgabegerät ansteuert.
- Vergewissern Sie sich, dass die Lautsprecher korrekt angeschlossen sind, wenn das Gerät kürzlich repariert oder aufgerüstet wurde.
- Probieren Sie es aus, Kopfhörer oder externe Boxen anzuschließen, wenn die internen Lautsprecher keinen Ton von sich geben. Funktionieren diese, besteht die Möglichkeit, dass die eingebauten Lautsprecher defekt sind. Je nachdem, wo genau diese angebracht sind, kann es leicht passieren, dass sie Feuchtigkeit abbekommen.
- Wenn Kopfhörer funktionieren, müssen Sie die internen Lautsprecher womöglich ersetzen. Vergewissern Sie sich, dass Ihr Gerät neu gestartet wurde, und überprüfen Sie noch einmal die Einstellungen für seine Ausgabe. Versuchen Sie auch, das Standardausgabegerät zu ändern oder zurückzusetzen und das Gerät zu deaktivieren und danach wieder zu aktivieren.

Eingaben werden nicht oder nicht richtig erkannt

- Bevor Sie davon ausgehen, dass ein Hardware-Problem vorliegt, sollten Sie sich vergewissern, dass das Gerät ansonsten einwandfrei arbeitet. Wenn das System »eingefroren« ist, scheinen auch die Eingabegeräte nicht oder nur fehlerhaft zu funktionieren. Lesen Sie im Abschnitt 23.5.1, *Stromversorgung und beeinträchtigte Leistung*, nach, um derartige Probleme zu beheben.
- Wenn keine der Tasten Ihres Laptops funktioniert, ist es gut möglich, dass sich das folienartige Flachbandkabel, über das die Tastatur mit dem Mainboard verbunden ist, durch einen Stoß oder Ruck ein wenig verschoben hat. Diese filigranen Anschlüsse sind relativ fragil und können schon mal verrutschen. Lesen Sie im Handbuch nach oder erkundigen Sie sich beim Hersteller, um den Anschluss gegebenenfalls neu auszurichten.

- Wenn Ziffern angezeigt werden, obwohl eigentlich Buchstaben zu erwarten wären, ist die Taste `Numlock` aktiviert. Deaktivieren Sie diese. Achten Sie auf die Zustandsanzeige für NUM LOCK (falls vorhanden).
- Laptop-Tastaturen werden häufig sehr viel stärker beansprucht als Desktop-Tastaturen. All die Treffen, die mit einem Mittagessen verbunden werden, all die Zusammenkünfte im Café, um Ideen zu sammeln ... In der Nähe einer Tastatur zu essen oder zu trinken schreit förmlich nach Problemen. Falls Ihre Tasten ein wenig klemmen, sollten Sie versuchen, die Tastatur mit Druckluftspray zu reinigen. Sind die Tasten, beispielsweise nach dem Verschütten von Limonade, so gravierend verklebt, dass der Einsatz von Lösungsmitteln geboten ist, müssen Sie die Tastatur vorher ausbauen. Stellen Sie nach der Reinigung unbedingt sicher, dass die Tastatur vollkommen trocken ist, bevor Sie diese wieder anschließen, da es anderenfalls zu Kurzschlüssen kommen kann.
- Bei einer einzelnen nicht funktionierenden Taste könnte diese leicht verrutscht sein und deshalb beim Betätigen keinen elektrischen Kontakt herstellen. Oft steht solch eine Taste ein wenig vor oder ist leicht verdreht und ist in diesem Zustand ziemlich empfindlich. Seien Sie also behutsam, wenn Sie es vermeiden möchten, Ersatz beschaffen zu müssen. Finden Sie heraus, welche Art Schalter die Tastatur verwendet, und nehmen Sie bitte zur Kenntnis, dass eine Tastatur durchaus mehrere verschiedene Schaltertypen verwenden kann. Versuchen Sie, eine schrittweise Anleitung zum Ablösen und Befestigen der Tasten für das betroffene Gerät zu finden. Falls Sie solch eine Anleitung nicht finden können, sollten Sie nach einer allgemeinen Anleitung zur Handhabung des Schaltertyps suchen, bevor Sie fortfahren.
- Falls Probleme mit dem Touchpad oder den Tasten unterhalb des Touchpads auftreten, wirkt etwas Druckluft manchmal Wunder, weil dadurch Verunreinigungen durch Staub, Essensreste oder Tierhaare beseitigt werden. Oft ist die Druckluft sehr viel wirksamer, wenn Sie die Tastatur vorher entfernen. Seien Sie dabei aber behutsam und beachten Sie die Anweisungen des Herstellers.
- Gegebenenfalls möchten Sie anschließend die Touchpad-Einstellungen neu konfigurieren. Dazu können Sie unter Windows in der Systemsteuerung das Applet MAUS und in macOS die Systemeinstellung TRACKPAD verwenden.
- Falls der Touchscreen nicht richtig oder fehlerhaft reagiert, sollten Sie überprüfen, ob er verschmutzt, verschmiert oder durch Flüssigkeiten verunreinigt ist – die Sensoren spielen dann gern verrückt. Reinigen Sie den Bildschirm mit einem trockenen Mikrofasertuch.
- Manche Touchscreens scheinen fehlerhaft zu arbeiten, weil sie auf unbeabsichtigte Berührungen reagieren. Das Design einiger Geräte führt dazu, dass man es so hält, dass ein Teil der Hand oder des Arms sich zu nah am Rand des Bildschirms befindet. Unter Umständen wird das als Berührung interpretiert.
- Eventuell verfügt Ihr Gerät über Diagnosewerkzeuge zur Behebung von Problemen mit dem Touchscreen, die über das BIOS zugänglich sind. Lesen Sie in der Dokumentation des Herstellers nach, wie Sie darauf zugreifen können. Falls solche Werkzeuge vorhanden sind, können Sie damit schnell feststellen, ob Sie es mit einem Problem der Hardware oder der Konfiguration zu tun haben. Das Applet TABLET PC-EINSTELLUNGEN in der Systemsteuerung erlaubt es Ihnen, den Bildschirm zu kalibrieren oder auf Werkseinstellungen zurückzusetzen. In macOS gibt es die Systemeinstellung TRACKPAD. Versuchen Sie, den Touchscreen zurückzusetzen und ihn neu zu kalibrieren.

Wichtig

Das unter dem englischen Begriff *Ghost Cursor* bekannte Phänomen besitzt zwei Bedeutungen. Zum einen sind damit Phantombilder des Mauszeigers gemeint, die bei Mausbewegungen der tatsächlichen Position hinterhereilen. Oft ist das ein Anzeichen für einen älteren, etwas trägen Monitor, manchmal aber auch für eine fehlerhaft konfigurierte Bildwiederholrate. Zum anderen werden mit diesem Begriff unkontrollierte Sprünge der Mauszeigerposition bezeichnet, die auch ohne Berührung des Touchpads auftreten. Dieses Verhalten deutet auf eine Beschädigung des Touchpads hin, das unter Umständen ersetzt werden muss.

23.6 Wiederholung

23.6.1 Fragen

1. Welche der folgenden Maßnahmen sind beim Umgang mit Akkus sinnvoll? (Wählen Sie zwei Antworten aus.)
   A. Die Kontakte vorsichtig mit einem weichen Tuch und etwas Reinigungsalkohol säubern
   B. Bei längerer Nichtbenutzung in der Kühltruhe lagern
   C. Defekte Akkus über den Hausmüll entsorgen
   D. Lagerung an einem kühlen, trockenen Ort
2. Wie müssen Sie vorgehen, um die WLAN-Antenne eines Laptops zu ersetzen?
   A. Tastatur entfernen
   B. Bildschirm entfernen
   C. Abdeckplatte des Gerätebodens entfernen
   D. Das ist nicht möglich
3. An welche Busse werden ExpressCards angebunden? (Wählen Sie zwei Antworten aus.)
   A. ACPI
   B. PCI
   C. PCIe
   D. USB
4. Klaras Laptop verfügt über einen DVI-Anschluss, an den sie einen Projektor angeschlossen hat. Sie bereitet sich auf ihre Präsentation vor, aber auf der Leinwand erscheint kein Bild. Auf dem Laptop wird die Präsentation angezeigt und auch der Projektor scheint zu funktionieren, auf der Leinwand erscheint jedoch nur ein helles weißes Bild. Wo vermuten Sie das Problem?
   A. Klara muss den Projektor anschließen.
   B. Klara verwendet den Akku. Man muss den Laptop an das Stromnetz anschließen, um den DVI-Anschluss verwenden zu können.
   C. Klara muss die PC-Karten-Treiber aktualisieren, damit auch Projektoren unterstützt werden.
   D. Klara muss eine bestimmte Funktionstastenkombination auf ihrer Tastatur drücken, um den Anzeigemodus zu wechseln.
5. Was ist der wichtigste Vorteil, wenn bei einem Laptop mit Shared Memory der Arbeitsspeicher erweitert wird? (Wählen Sie die beste Antwort aus.)
   A. Längere Akkulaufzeit
   B. Bessere Systemleistung
   C. Bessere Grafikleistung
   D. Es gibt keinen Vorteil. Bei Systemen mit gemeinsam genutztem Speicher hat es keine Auswirkung, wenn mehr RAM eingebaut wird.
6. Welche Art von Bildschirmen verwenden tragbare Computer heutzutage für gewöhnlich? (Wählen Sie zwei Antworten aus.)
   A. Röhrenmonitor
   B. LCD
   C. OLED
   D. Plasma

7. Stefan beklagt sich, dass sein alter Laptop auch nach einer RAM-Aufrüstung noch ziemlich lahm ist. Wie lässt sich die Systemleistung verbessern?
   A. Noch mehr RAM aufrüsten
   B. Ersetzen des Netzteils
   C. Den Akku austauschen
   D. Die Festplatte durch eine SSD ersetzen
8. Johannes ist eigentlich sehr zufrieden mit seinem Laptop, kann aber nicht nachvollziehen, warum sein drahtloses Netzwerk im Vergleich mit den anderen Laptops so langsam ist. Sie stellen fest, dass eine 802.11n-Netzwerkkarte verbaut ist. Wie lässt sich die Verbindungsgeschwindigkeit erhöhen?
   A. Mehr RAM einbauen
   B. Einen Bildschirm mit besserer Antenne verwenden
   C. Die 802.11n-Mini-PCIe-Netzwerkkarte durch eine 802.11ac-Karte ersetzen
   D. Johannes braucht einen neuen Laptop. Hier lässt sich nichts verbessern.
9. Nachdem der kleine Sohn eines Kunden mit Filzstiften und Edding auf dem Bildschirm herumgemalt hat, sah er sich gezwungen, den Bildschirm auszutauschen. Kurz darauf meldet sich der Kunde erneut und beschwert sich, dass sein drahtloses Netzwerk nicht mehr funktioniert. Was könnte dieses Problem verursachen?
   A. Es gibt hier keinen Zusammenhang, daher kommen verschiedene Ursachen infrage.
   B. Der Kunde hat wohl versehentlich die Verbindung zwischen der 802.11-Mini-PCIe-Karte und der Antenne getrennt.
   C. Der Kunde hat einen Bildschirm ohne Antenne eingebaut.
   D. Der Kunde hat vermutlich vergessen, das Antennenkabel des neuen Bildschirms an die Netzwerkkarte anzuschließen.
10. Ein Benutzer mit einem nagelneuen Laptop ruft Christian an und beklagt sich, dass er unter Kopfschmerzen leidet, seitdem er das neue Gerät benutzt. Was ist Ihrer Meinung nach die Ursache?
   A. Der Plasma-Bildschirm
   B. Der Röhrenbildschirm
   C. Der LED-Bildschirm mit heruntergeregelter Helligkeit
   D. Der LED-Bildschirm mit voller Helligkeit

23.6.2 Antworten

1. **A, D.** Theoretisch ist es denkbar, einen Akku in der Gefriertruhe zu lagern, in der Praxis gilt das aber nicht. Alle Akkus enthalten giftige Chemikalien und sollten keinesfalls wie Hausmüll behandelt werden.
2. **B.** Die WLAN-Antenne befindet sich neben dem Display, deshalb muss der Bildschirm entfernt werden, oder zumindest der Einbaurahmen.
3. **C, D.** ExpressCards werden per PCI Express oder USB angeschlossen.
4. **D.** Klara muss eine bestimmte Funktionstastenkombination auf ihrer Tastatur drücken, um den Anzeigemodus zu wechseln.
5. **B.** Wenn bei einem Laptop mit Shared Memory der Arbeitsspeicher erweitert wird, steigt die Systemleistung insgesamt.
6. **A, B.** Aktuelle Laptops besitzen LCD-Bildschirme (auch wenn manche als LED-Bildschirme vermarktet werden).

7. **D.** Das Ersetzen der Festplatte durch eine SSD beschleunigt das System.
8. **C.** Die 802.11n-Karte sollte durch eine 802.11ac-Karte ersetzt werden.
9. **D.** Eine nicht verbundene Antenne führt dazu, dass das drahtlose Netzwerk nicht funktioniert.
10. **C.** Beim Absenken der Helligkeit von LED-Bildschirmen kann es zum Flackern des Bildschirms kommen.

Mobile Geräte | 24

Themen in diesem Kapitel:

- Funktionen und Leistungsvermögen von mobilen Geräten
- Die wichtigsten Betriebssysteme für mobile Geräte
- Konfiguration von mobilen Geräten

Es ist kaum vorstellbar, dass es vor rund zehn Jahren noch keine mobilen Geräte wie das beliebte iPhone oder Mobiltelefone mit Android gab. Smartphones, Tablets und inzwischen auch Smartwatches ermöglichen es den Menschen, fast überall auf das Internet zuzugreifen, und sie können dank dieser Geräte selbst unterwegs wichtige Aufgaben erledigen.

So erstaunlich diese mobilen Geräte auch sind: Es ist gar nicht so einfach, eine Definition dafür zu finden, die allgemeine Zustimmung findet. Wenn Sie Leute fragen, die im Umgang mit solchen Geräten Erfahrung haben, bekommen Sie vielfältige Beschreibungen der Funktionalität und der Fähigkeiten zu hören, aber keine *Definition*. Die folgenden Aspekte machen mobile Geräte im engeren Sinn aus (und selbst diese sind nicht völlig unumstritten):

- Leichtgewichtig, für gewöhnlich deutlich weniger als ein Kilogramm
- So klein, dass man sie in der Hand halten oder in der Hosentasche bei sich tragen kann
- Touchscreen oder Stiftbedienung; keine Tastatur und keine Maus
- Kompaktgeräte ohne austauschbare Ersatzteile
- Kein Desktop-OS, sondern speziell für mobile Geräte angepasste Betriebssysteme

Letzteres ist von besonderer Bedeutung, weil sich dadurch klassische Laptops, die kaum größer als ein Tablet sind, leicht von mobilen Geräten im engeren Sinn abgrenzen lassen. Auf einem typischen Laptop läuft ein Desktop-OS wie Windows, macOS oder eine Linux-Distribution wie Ubuntu. Auf einem mobilen Gerät im engeren Sinn hingegen läuft Apple iOS oder Google Android.

In diesem Kapitel wollen wir uns diese mobilen Geräte genauer ansehen. Zunächst betrachten wir die Funktionen und Fähigkeiten der im mobilen Marktsegment gebräuchlichen Geräte. Danach betrachten wir die Betriebssysteme für mobile Geräte. Abschließend kommen die Einzelheiten bei der Konfiguration für den persönlichen Gebrauch zur Sprache. Die Fehlerbehebung und die Sicherheitsaspekte hebe ich mir für Kapitel 25 auf. Die CompTIA A+-Prüfungen haben so einiges über mobile Geräte zum Inhalt und es gibt eine Menge zu erörtern, legen wir also los!

1001

24.1 Kategorien mobiler Geräte

Die spezialisierte Hardware der mobilen Geräte legt weitgehend fest, über welche Fähigkeiten sie verfügen. Im ersten Abschnitt erläutere ich die verschiedenen Formfaktoren und untersuche die Hardwarekomponenten, die in den meisten Geräten vorhanden sind.

24.1.1 Gerätevarianten

Die aktuellen mobilen Geräte können in verschiedene Kategorien unterteilt werden, wie Smartphones, Tablets, Wearables und sonstige mobile Geräte, die alle über ähnliche Funktionen und Fähigkeiten verfügen. Darüber hinaus gibt es einige weitere Geräte, die vor allem eine ganz bestimmte

Aufgabe besser als ein Allzweckgerät wie ein Smartphone oder ein Tablet erfüllen sollen. E-Book-Lesegeräte sind hierfür ein gutes Beispiel. Die Lernziele der CompTIA A+-Prüfung enthalten eine ziemlich lange Liste von Geräten, die wir uns nun der Reihe nach ansehen, um zu verstehen, was sie leisten können. Fangen wir mit dem verbreitetsten Gerätetyp an, dem Smartphone.

Smartphones

Zu den ersten mobilen Geräte gehörten die sogenannten *PDAs* (*Personal Digital Assistants*), wie z.B. der Compaq iPaq, der Ende der 1990er-Jahre auf den Markt kam. PDAs besaßen die grundlegenden Funktionen der heutigen Geräte, verfügten jedoch über keine Mobilfunkverbindung – telefonieren konnte man damit nicht. Viele Leute (mich eingeschlossen) trugen fast zehn Jahre lang sowohl ein Mobiltelefon als auch einen PDA mit sich herum und fragten sich, wann denn wohl jemand auf die Idee kommt, die beiden zu vereinen. Ab etwa 2003 bis 2005 wurden die ersten PDAs vorgestellt, die gleichzeitig ein Mobiltelefon waren. (Die wirklich interessanten Funktionalitäten, wie der Zugriff auf Daten im Internet, waren damals allerdings kaum vorhanden.) Abbildung 24.1 zeigt einen der ersten PDAs mit eingebautem Mobiltelefon, den seinerzeit sehr beliebten RIM Blackberry.



Abb. 24.1: RIM Blackberry (Foto mit freundlicher Genehmigung von TotalSem Tech Museum)

Solche Geräte waren für die damaligen Verhältnisse ziemlich leistungsfähig, aber erst als Apple 2007 das iPhone vorstellte (Abbildung 24.2), konnte man erstmals all das sehen, was heute ein modernes Smartphone ausmacht:

- Eine Multitouch-Bedienoberfläche als primäre Eingabemethode bei der Verwendung des Smartphones
- Eine hochgradig standardisierte API (*Application Programming Interface*), die es Entwicklern ermöglicht, neue Apps für das System zu programmieren
- Nahtlose Einbindung der Mobilfunkverbindung, die es beliebigen Anwendungen (Browsern, E-Mail-Clients, Spielen usw.) gestattet, über das Internet Daten auszutauschen
- Ein Vertriebskanal, der es Benutzern erlaubt, neue Apps zu installieren und ein Werkzeug zur Synchronisierung bzw. Sicherung von Daten



Abb. 24.2: Eins der ersten iPhones

Seither wurden Smartphones kontinuierlich weiterentwickelt und es gibt viele weitere Werkzeuge, Anwendungen und Features. Smartphones sind in den letzten Jahren nahezu allgegenwärtig geworden und wir gehen ganz selbstverständlich davon aus, mit unseren Geräten immer und überall mittels Mobilfunkverbindungen auf unsere Daten und Inhalte zugreifen zu können. Man kann mit Smartphones viel mehr anfangen, als nur Anrufe zu tätigen oder entgegenzunehmen. Wir surfen mit ihnen im Internet, hören Musik, betrachten Videos, senden und empfangen E-Mail und nutzen sie sogar geschäftlich. Aus diesem Grund muss die Infrastruktur, über die Smartphones und Daten miteinander verbunden sind, schnell, stabil und sicher sein.

Auf den meisten Smartphones läuft eins der beiden »großen« Betriebssysteme: Apple iOS oder Google Android (Abbildung 24.3). iOS läuft nur auf Hardware von Apple, wie dem iPhone. Mobiltelefone, auf denen Android, gibt es von einer Vielzahl von Herstellern. Smartphones besitzen im Allgemeinen keine vom Endbenutzer austauschbaren Teile und müssen zur Reparatur in darauf spezialisierte (und teilweise autorisierte) Werkstätten gegeben werden.





Abb. 24.3: Die beiden »großen« Smartphone-Betriebssysteme: Android (links) und iOS (rechts)

Tablets

Tablets haben große Ähnlichkeit mit Smartphones: Auf ihnen läuft das gleiche Betriebssystem, sie verwenden die gleichen Multitouchscreens und können auch die gleichen Apps ausführen. Aus rein technischer Sicht handelt es sich um große Smartphones ohne den Telefonteil. Die Bildschirmdiagonale gängiger Smartphones beträgt etwa 5 Zoll (knapp 13 cm), diejenige von Tablets typischerweise 7 bis 12,9 Zoll (etwa 18 bis 33 cm, siehe Abbildung 24.4).



Abb. 24.4: Ein typisches Tablet

Im Gegensatz zu Smartphones besitzen Tablets im Allgemeinen keinen Mobilfunkzugang (wenngleich es einige Ausnahmen gibt) und verwenden WLAN nach dem 802.11-Standard, um auf Netzwerke zuzugreifen. Es gibt sehr preiswerte Tablets mit bescheidener Hardware, auf denen zumeist eine Android-Variante läuft, und natürlich die High-End-Tablets, wie das iPad von Apple. Die Unterschiede zwischen dem unteren und dem oberen Ende des Preisspektrums betreffen Hardwarequalität, Fähigkeiten und Funktionalitäten.

Zweckgebundene mobile Geräte

In der Einleitung habe ich Geräte erwähnt, die eine ganz bestimmte Aufgabe erfüllen sollen. Sie sind speziell dafür ausgelegt, eine Aufgabe besonders gut zu erledigen, die sich im Prinzip auch mit einem Smartphone oder Tablet erledigen ließe. Damit ergeben sich einige interessante Aspekte. Zum einen nutzen Allzweckgeräte zur Erledigung der Aufgabe eine App. Zum anderen ist die Daseinsberechtigung für zweckgebundene Geräte tendenziell im Laufe der Zeit immer weniger erkennbar, weil die Allzweckgeräte die Aufgabe immer besser erledigen, aber den Vorteil haben, dass man nur ein Gerät braucht. Reine MP3-Player sind ein gutes Beispiel für zweckgebundene Geräte, die Smartphones zum Opfer gefallen sind.

Die CompTIA verlangt von Ihnen, dass Sie zwei dieser Gerätetypen kennen: E-Book-Lesegeräte und GPS-Empfänger. Weil GPS-Empfänger genau auf die namensgebenden Hardwarekomponenten zugeschnitten sind, betrachten wir sie im nachfolgenden Abschnitt 24.1.2, *Funktionen der Hardware*, wenn wir uns mit GPS befassen. Hier sehen wir uns E-Book-Lesegeräte an, die man eher als kleine Tablets betrachten kann, die für das Lesen maßgeschneidert sind.

E-Book-Lesegeräte Wie Sie sich denken können, erlauben E-Book-Lesegeräte die Anzeige elektronischer Bücher (E-Books). Viele E-Book-Lesegeräte nutzen eine energiesparende Technologie zur Anzeige von Graustufengrafik namens *ePaper*. Sie bieten eine einfache Schnittstelle zum Zugriff auf E-Books, zur Navigation beim Lesen und Durchführung damit zusammenhängender Aufgaben wie

Texthervorhebungen, das Anlegen von Lesezeichen, das Teilen von Textabschnitten oder das Nachschlagen von Definitionen. Ursprünglich besaßen die Geräte physische Tasten, aber im Laufe der Zeit verwendeten immer mehr Geräte zur Bedienung einen Touchscreen, so wie der Kindle Paperwhite von Amazon in Abbildung 24.5.

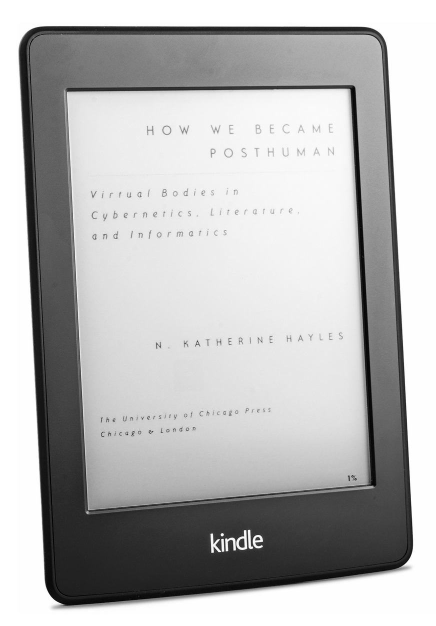


Abb. 24.5: Das E-Book-Lesegerät Kindle Paperwhite

Allmählich entwickelten sich E-Book-Lesegeräte immer weiter in Richtung eines vollwertigen Tablets. Die Produktreihen Nook von Barnes und Noble und Kindle von Amazon waren anfangs einfache Schwarz-Weiß-Geräte, die aktuellen Modelle hingegen sind vollwertige Tablets. Tablets sind zwar für allgemeine Aufgaben und Medienkonsum besser geeignet, der große Vorteil von E-Book-Lesegeräten gegenüber Tablets besteht jedoch darin, dass der Bildschirm nicht für Spiele oder das Betrachten von Videos, sondern speziell für das Lesen bei ungünstigen Umgebungsbedingungen ausgelegt ist, beispielsweise bei sich stark ändernden Lichtverhältnissen oder sehr heller Umgebung, und sich automatisch an die Beleuchtung anpasst. Die Akkulaufzeit bemisst sich daher in Tagen oder Wochen. Sowohl Kindle als auch Nook bieten Apps zum Lesen von E-Books für andere Plattformen an. Ebenso wie die eigenständigen E-Book-Lesegeräte können sich diese Apps mit dem Online-Buchladen verbinden, E-Books herunterladen und die Bibliothek des Benutzers verwalten.

Wearables

Der große Nachteil von mobilen Geräten ist, dass sie praktisch nutzlos sind, wenn Sie sie nicht in Händen halten. Unser Verlangen nach Daten hat einen Anreiz dafür geschaffen, uns die Daten durch Wearables näherzubringen. Dabei handelt es sich um kleine Computersysteme, die in der Kleidung oder am Körper getragen werden. Wearables gibt es schon seit einigen Jahren, aber erst seit es die kürzlich auf den Markt gekommenen Smartwatches wie die Apple Watch oder Armbanduhren mit Android Wear OS gibt, zeigt sich, dass sich die bedeutenden Hersteller Wearables zu eigen machen.

Wearables unterscheiden sich in vielerlei Hinsicht von anderen mobilen Geräten:

- Sie sind sehr klein und sehr leicht; nicht selten wiegen sie nur ein paar Dutzend Gramm.
- Die Anzeigen sind ebenfalls klein. Die Bildschirmdiagonale beträgt nur 2 Zoll (ca. 5 cm) oder oft auch deutlich weniger.

- Sie verwenden leichtgewichtige Betriebssysteme, die nur eine Teilmenge der Funktionen eines typischen Smartphone-Betriebssystems beherrschen.
- Die Leistungsfähigkeit der Hardware ist begrenzt, allerdings finden sich häufig Beschleunigungssensoren (zum Einsatz als Schrittzähler).
- Sie müssen mit einem anderen Gerät gekoppelt werden, für gewöhnlich mit einem Smartphone.

In den Lernzielen der CompTIA A+-Prüfung werden drei Wearables ausdrücklich erwähnt: Smartwatches, Fitness-Armbänder und VR/AR-Headsets. Sehen wir uns diese Geräte genauer an.

Wichtig

Wearables sollen Smartphones nicht ersetzen, sondern nur bestimmte einfache Aufgaben erledigen. Für viele Funktionen sind Wearables ungeeignet. Falls Sie sich fragen, warum Wearables wie Fitness-Armbänder nicht den eben erwähnten zweckgebundenen mobilen Geräten zugeordnet werden: Der Unterschied besteht darin, dass Letztere eigenständig arbeiten.

Smartwatches

Die Smartwatch minimiert den Aufwand, der mit häufigen Aufgaben des Smartphones einhergeht, wie den Empfang von Benachrichtigungen aller Art, die Anzeige von Uhrzeit und Wettervorhersage, die Wiedergabe von Musik oder die Aufzeichnung von Fitnessdaten. Abbildung 24.6 zeigt eine typische Smartwatch, die Apple Watch.



Abb. 24.6: Apple Watch

Fitness-Armbänder

Eine stetig wachsende Zahl von Fitness-Armbändern möchte Ihnen dabei helfen, Ihre Ziele bei der körperlichen Ertüchtigung zu erreichen. Die gängigen Modelle zählen mittels eines Accelerometers Ihre Schritte, messen mithilfe eines Sensors Ihren Puls, nutzen GPS, um Ihre Position beim Laufen zu verfolgen und erinnern Sie per Vibrationsalarm daran, sich in Bewegung zu setzen. Neben Fitness-Armbändern, die wie eine Armbanduhr getragen werden, gibt es auch kleine Geräte in Form eines Schlüsselanhängers, die mit einer Klammer an der Kleidung befestigt werden. Diese Geräte können meist aber nicht viel mehr als Schritte zu zählen. Armbänder, wie das viel genutzte Fitbit Surge des Autors (Abbildung 24.7), bieten darüber hinaus Features wie GPS und Pulsmessung.



Abb. 24.7: Mikes ramponiertes Fitness-Armband

VR/AR-Headsets

Headsets bieten viele Möglichkeiten der Computernutzung. Gefällt Ihnen diese vage Aussage? Hier sind die Details. Es gibt verschiedene Varianten. Die häufigste ist kein computerähnliches Gerät, sondern Lautsprecher und Mikrofon, die für das Chatten mit dem Computer ausgelegt sind (per Voice over IP oder Skype, siehe Kapitel 21). Abbildung 24.8 zeigt ein typisches Headset.



Abb. 24.8: Typisches Headset zum Chatten

Es gibt jedoch auch zwei sehr unterschiedliche computerähnliche Varianten. Die eine ist für VR (Virtuelle Realität) und die andere für AR (*Augmented Reality*, erweiterte Realität) ausgelegt. VR-Headsets, die Ihnen den Zugang zu einer dreidimensionalen Welt verschaffen, habe ich in Kapitel 17 bereits erörtert. Mit hochwertiger Hardware und der entsprechenden VR-Software können Sie vom Sofa aus die erstaunlichsten Orte erkunden. Abbildung 24.9 zeigt einen Mitarbeiter, der die neueste VR-Technologie nutzt, um das im Orbit befindliche virtuelle Hauptquartier von Totalsem zu erkunden.



Abb. 24.9: Spieler mit VR-Headset (der gar nicht bemerkt, wie albern er aussieht)

Die *erweiterte Realität* (AR) bietet das, was der Begriff schon besagt, nämlich zusätzliche Elemente, die Sie mit Ihren Augen sehen oder mit Ihren Ohren hören können. AR versetzt Sie nicht in eine künstliche Welt, sondern ergänzt das, was Sie mit Ihren physischen »Eingabegeräten« (soll heißen: Augen und Ohren) wahrnehmen, um erstaunliche Details. Hier ist ein profanes, aber cooles Beispiel: Das schwedische Möbelhaus IKEA bietet eine App namens *IKEA Place* an, die es Ihnen ermöglicht zu betrachten, wie ein Möbelstück in Ihrer aktuellen Umgebung aussieht. Abbildung 24.10 zeigt beispielsweise das leere Esszimmer meines Redakteurs Scott, in dem er mit einem iPhone per AR einen Esstisch und Stühle platziert hat.



Abb. 24.10: AR-App von IKEA

AR-Headsets kombinieren Displays und Kameras in einem Gerät. Eines der ersten AR-Headsets war *Google Glass*. Es besaß eine eingebaute Kamera und beherrschte Bluetooth-Verbindungen. Damit war es möglich, Bilder und Videos aus der Ich-Perspektive aufzunehmen. Außerdem konnte das Gerät via Bluetooth mit dem Smartphone gekoppelt werden, wodurch es möglich war, Anrufe entgegenzunehmen und sich auf der Brille Informationen anzeigen zu lassen.

Wie sich herausstellen sollte, bestand die große Schwierigkeit darin, dass die Leute Ihre Privatsphäre verletzt sahen. Dass es für den Träger einer Google Glass problemlos möglich war, seine Umgebung zu fotografieren oder zu filmen, oft ohne dass es die Anwesenden bemerkten, wurde von vielen Leuten als unangenehmes Eindringen in die eigene Privatsphäre empfunden. Tatsächlich wurde von vielen Restaurants, Bars und anderen öffentlich zugänglichen Einrichtungen die Verwendung von Google Glass in den eigenen Räumlichkeiten untersagt.

Eine neue Generation von AR-Headsets konzentriert sich mehr auf eine Zielgruppe, die einem bestimmten Hobby nachgeht oder über besondere Fähigkeiten verfügt. Die Headsets Garmin Varia Vision, Solos Smart Glasses und Everysight Raptor AR beispielsweise ermöglichen es Radfahrern, Geschwindigkeit, Trittfrequenz, Puls, zurückgelegte Strecke, verbrannte Kalorien, Höhe über dem Meeresspiegel und vieles mehr aufzuzeichnen. Die Geräte lassen sich ebenfalls mit dem Smartphone synchronisieren, sodass Sie eine Statistik erstellen können. Manche dieser Geräte können sich mit anderen mobilen Geräten verbinden, um die Umgebung zu überwachen, sodass Sie beispielsweise gewarnt sind, wenn eine Kollision mit anderen Fahrzeugen droht.

24.1.2 Funktionen der Hardware

Die Hardware der mobilen Geräte ermöglicht eine Vielzahl verschiedener Funktionen. In diesem Abschnitt kommen Bildschirmtechnologien, Kameras, Mikrofone, Digitizer und GPS zur Sprache.

Bildschirmtechnologie

Bei mobilen Geräten werden die verschiedensten Bildschirmtypen verwendet. Die meisten Tablets besitzen LCD-Panels vom gleichen Typ, wie sie in Laptops und Desktops eingesetzt werden. Preiswertere Geräte verwenden *Twisted Nematic* (TN), während die besseren, wie Apples iPad, *In-Plane-Switching* (IPS) einsetzen, um einen höheren Sichtwinkel und sattere Farben zu erzielen. In Kapitel 17 können Sie die Unterschiede zwischen den Displaytypen nachlesen. Im Abschnitt *Digitizer* betrachten wir die Technologie, die aus den Bildschirmen Touchscreens macht.

Einige kleinere Geräte, etwa höherwertige Smartphones, nutzen eine verwandte Technologie namens *OLED* (*Organic Light-Emitting Diode*), bei der organische Verbindungen das Licht liefern. Fließt elektrischer Strom, leuchten in der organischen Schicht nur genau definierte Punkte auf. Einige Geräte verwenden Aktivmatrix-OLEDs (AMOLED), die eine zusätzliche TFT-Schicht besitzen, um den Bildschirm besser ansteuern zu können. Bei OLEDs und AMOLEDs gibt es keine Hintergrundbeleuchtung, daher können sie echtes Schwarz darstellen, sind leichter und verbrauchen weniger Energie als alle LCD-Technologien.

Wichtig

Bei OLED-Bildschirmen fließt zur Lichterzeugung elektrischer Strom durch organische Verbindungen. Sie besitzen keine Hintergrundbeleuchtung.

Kameras

Viele mobile Geräte besitzen zwei Kameras, von denen eine auf den Benutzer blickt und die andere von ihm fort. Dank dieser Kameras können Sie per Facetime mit Oma chatten, tränenreiche Geständnisse zur Veröffentlichung auf YouTube filmen und Instagram-Selfies erstellen! Die Kameras können Ihre Aufnahmen über Mobilfunk und IP-basierte Netze wie das Internet übertragen.

Die neueste Kamera-Generation, die insbesondere in Smartphones verbaut wird, kann herkömmlichen Kameras inzwischen durchaus das Wasser reichen oder diese sogar übertreffen (Abbildung 24.11).



Abb. 24.11: Die Kamera-App des Autors auf einem iPhone XS

Aktuelle Smartphone-Kameras verfügen über Features wie *HDR* (*High Dynamic Range*, ein Verfahren, mit dem sich große Helligkeitsunterschiede detailreich wiedergeben lassen) und Lichtwechselausgleich, die es dem Benutzer gestatten, Bilder und Videos sehr fein auf die Lichtverhältnisse abzustimmen. Darüber hinaus bieten die Kameras eine Reihe von Optionen bei der Aufnahme von Fotos oder Videos. Einige Kameras ermöglichen es, Serienfotos aufzunehmen (z.B. mit zehn Bildern pro Sekunde), damit sie sich schnell bewegende Objekte richtig erfassen, oder können Zeitlupenvideos aufnehmen. In Kombination mit der Vielzahl von Apps zum Manipulieren und Filtern von Aufnahmen können Sie unterwegs Bilder bearbeiten, bereinigen und sogar Spezialeffekte hinzufügen.

Mikrofone

Fast alle mobilen Geräte besitzen ein Mikrofon – ein Smartphone ohne Mikrofon ergäbe auch kaum einen Sinn und Sie könnten Skype oder FaceTime nur unter großen Schwierigkeiten verwenden. Darüber hinaus nutzen viele Anwender ihr Smartphone für Sprachaufzeichnungen oder andere Audioaufnahmen. Die Mikrofone von Smartphones erledigen also durchaus mehrere Aufgaben.

Ebenso wie die im letzten Kapitel erörterten tragbaren Computer verfügen auch mobile Geräte oft über mehrere Mikrofone, die der Unterdrückung von Nebengeräuschen dienen. Bei mobilen Geräten müssen Sie jedoch, anders als bei klassischen tragbaren Computern, womöglich darauf achtgeben, keines der Mikrofone abzudecken.

Digitizer

Wenn Elektrotechniker von einem Digitizer sprechen, meinen sie damit ein elektronisches Bauteil, das analoge Signale in digitale umwandelt, diese also digitalisiert. Wir bezeichnen mit diesem Begriff im Zusammenhang mit mobilen Geräten jedoch etwas anderes. *Digitizer* bezieht sich auf den berührungsempfindlichen Bildschirm, also sozusagen auf den »Touch«-Teil des Touchscreens. Wenn Ihr Finger den Bildschirm berührt, registriert das feine, aus Sensoren bestehende Netz des Digitizers, das sich unter der Glasoberfläche befindet, an welcher Bildschirmposition sich ihr Finger befindet und meldet dies dem Betriebssystem. Ebenso wie bei modernen Trackpads können Sie bei den meisten Touchscreens einen oder mehrere Finger zur Bedienung verwenden.

GPS

Eine der wichtigsten Funktionen aktueller mobiler Geräte ist die Fähigkeit, den Aufenthaltsort des Geräts mittels *GPS* (*Global Positioning System*), Mobilfunknetz oder WLAN zu ermitteln. Dank der *Ortungsdienste* kann der Benutzer Geschäfte oder Restaurants in seiner Nähe finden oder feststellen, wo sich die nächste U- oder S-Bahnstation oder eine Bushaltestelle befindet. In diesem Abschnitt betrach-

ten wir, welche Möglichkeiten sich z.B. einem Smartphone dank der GPS-Fähigkeiten bieten, was eigenständige GPS-Empfänger leisten und was hinsichtlich des Datenschutzes bei Ortungsdiensten zu beachten ist.

Ein schönes Beispiel ist die Navigations-App *Waze* (Abbildung 24.12). Waze dient nicht nur zur Navigation, sondern stellt auch die von den Benutzern gesammelten Informationen über die aktuelle Verkehrslage zur Verfügung.

Eine weitere coole GPS-Anwendung ist die Suche nach dem Gerät, z.B. wenn es gestohlen wurde. Auf dem iPhone steht hierfür beispielsweise die App MEIN IPHONE SUCHEN zur Verfügung (Abbildung 24.13). Dieses Feature ist Teil der iCloud-Dienste, die allen iOS-Geräten kostenlos zur Verfügung stehen.

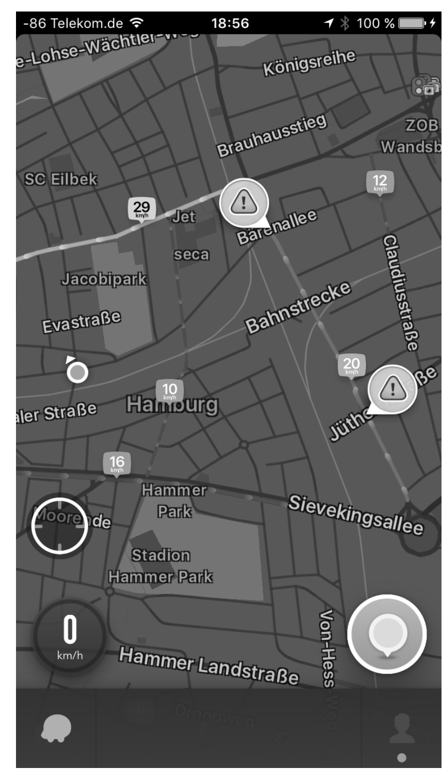


Abb. 24.12: Waze in Aktion

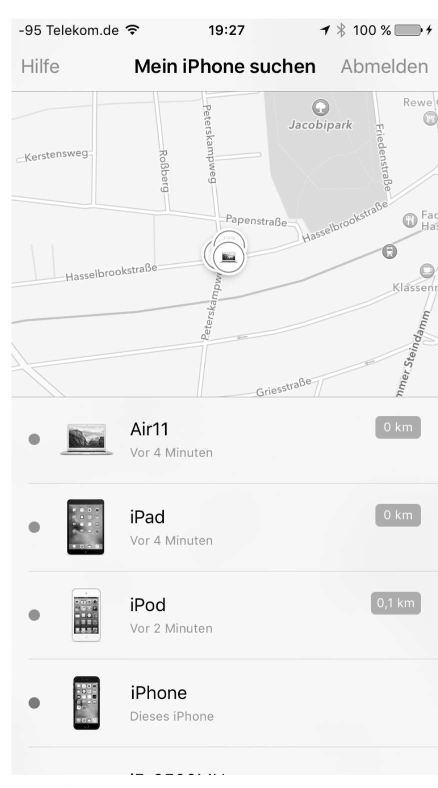


Abb. 24.13: Die App MEIN IPHONE SUCHEN

Eigenständige GPS-Empfänger Neben diesen Anwendungen der GPS-Technologie für Smartphones gibt es auch eine Vielzahl zweckgebundener GPS-Geräte. Am bekanntesten dürften die Navigationsgeräte sein, die an der Windschutzscheibe oder am Armaturenbrett eines Autos befestigt werden. Sie können sich sicherlich vorstellen, dass eine solche Navigationshilfe auch für andere Fahrzeuge nützlich ist, wie etwa Schiffe, Flugzeuge oder Fahrräder. Es gibt auch tragbare Navigationsgeräte, die man zur Ortung verwenden kann, wenn man kein Fahrzeug benutzt. So gibt es beispielsweise spezielle Geräte für Taucher, Radfahrer, Jäger und so weiter.

GPS-fähige Smartphones sind zur alltäglichen Navigation in zivilisierter Umgebung völlig ausreichend, aber die spezialisierten Geräte bieten besser an den Nischenbedarf angepasste Funktionen, wie z.B. spezielle Landkarten, zusätzliche Sensoren für bestimmte Zwecke, Aufzeichnung der Wegstrecke oder Lesezeichen für aufgesuchte Orte. Andere Geräte sind besonders stoßfest, wasserdicht, energiesparend oder ermöglichen einen einfachen Austausch des Akkus.

Ortungsdienste und Datenschutz Dass Ihr Aufenthaltsort jederzeit festgestellt werden kann, ist im Allgemeinen eine feine Sache – wenn Sie denn damit einverstanden sind. Alle Betriebssysteme für mobile Geräte verfolgen standardmäßig Ihre aktuelle Position und speichern diese Daten oft über einen längeren Zeitraum. Wenn Ihnen das nicht ganz geheuer ist, können Sie es abschalten. Abbildung 24.14 zeigt, wie die Ortungsdienste auf einem iPhone deaktiviert werden.



Abb. 24.14: Ortungsdienste deaktivieren

Wichtig

Die GPS-Fähigkeiten mobiler Geräte sind ein zweischneidiges Schwert. Die mit dem Internet oder dem GPS-Netzwerk verbundenen Geräte sind anhand bestimmter Merkmale wie IMEI-Nummer (*International Mobile Equipment Identity*) oder MAC-Adresse identifizierbar. Netzwerkbetreiber und staatliche Sicherheitsdienste können daher prinzipiell jederzeit feststellen, wo Sie sich gerade aufhalten. Dieses als *Geotracking* bezeichnete Lokalisierungsverfahren besitzt ein ziemlich großes Missbrauchspotenzial.

1002

24.2 Betriebssysteme für mobile Geräte

Zwei Betriebssysteme dominieren bei mobilen Geräten: Apple iOS und Google Android. Dieser Abschnitt beschreibt die Entwicklung und die Implementierung dieser Betriebssysteme und einige der wichtigsten Eigenschaften sowie die Funktionsweise der zugehörigen App-Stores.

24.2.1 Entwicklungsmodelle

Bevor wir uns im Detail mit den Betriebssystemen beschäftigen, sollten wir einen Blick auf das Gesamtbild werfen. Die verschiedenen Philosophien, die den Betriebssystemen zugrunde liegen, an denen sich auch ihre Hersteller orientieren, erklären, warum sie bestimmte Dinge auf die eine oder andere Art und Weise erledigen. Wir werfen zunächst einen Blick auf die Entwicklungsmodelle Closed Source und Open Source. Sie kennen diese Begriffe vermutlich, die beschreiben, wie Software veröffentlicht und lizenziert wird. (Sollte das nicht der Fall sein: In Kapitel 27 wird erläutert, wie sie auf Lizenzierung anwendbar sind.) Sie legen die Rahmenbedingungen für die Entwicklung und Veröffentlichung von Produkten fest. Anschließend betrachten wir, was diese Entwicklungsmodelle für Betriebssysteme bedeuten.

Closed Source

Das *Closed-Source*-Entwicklungsmodell kann man sich als eine Umschreibung der traditionellen Vorgehensweise vorstellen, ein Produkt herzustellen und zu verkaufen, ohne zu verraten, wie man es

gemacht hat. Dieses Modell erscheint einleuchtend, jedenfalls in unserer Kultur. Das Herstellungsverfahren ist ein Geschäftsgeheimnis, das Ihnen einen Wettbewerbsvorteil verschafft. Es zu verraten, könnte der Konkurrenz ermöglichen, Ihr Design zu kopieren, oder potenzielle Kunden auf den Gedanken bringen, das Produkt selbst herzustellen.

Herstellerspezifisch und proprietär Man verwendet manchmal die Begriffe *herstellerspezifisch* oder *proprietär* für ein Closed-Source-Produkt oder eine Closed-Source-Technologie, vor allem, wenn man darauf aufmerksam machen möchte, dass etwas keine gebräuchlichen, offenen Standards verwendet. Die Begriffe hängen mit dem Ausdruck *Closed Source* zusammen, dürfen aber nicht damit verwechselt werden, denn sie sind nicht synonym. Diese Bezeichnungen bedeuten oft, dass ein Produkt nicht vernünftig mit anderen Produkten zusammenarbeitet, weil es beispielsweise Stecker oder Kabel verwendet, die schwer erhältlich oder teuer sind, nicht für experimentierfreudige Benutzer geeignet ist, sich kaum reparieren lässt oder eine Menge anderer Probleme bereitet.

Was die Verwendung dieser Begriffe genau bedeutet, ist manchmal unklar. Wie Sie noch sehen werden, verwenden manche Hersteller einen gebräuchlichen Standard, wie z.B. USB 3.0, entwickeln aber einen eigenen Stecker. Rein technisch gesehen nutzt der Hersteller den offenen USB-Standard, dennoch bezeichnet man den Anschluss oder das Kabel des Geräts als proprietär.

Open Source

Sie können sich ein Produkt als Open Source im weiteren Sinne vorstellen, wenn der Entwickler eine Anleitung zur Herstellung veröffentlicht. Dabei muss es sich nicht unbedingt um Software handeln (wenngleich das meistens der Fall ist). Wenn ein Unternehmen ein Produkt als Open Source veröffentlicht, muss es anders vorgehen als Unternehmen, die das Closed-Source-Modell verwenden. Beispielsweise ist die Geheimhaltung bei diesem Modell von geringerer Bedeutung. Wenn dem Unternehmen klar ist, dass jeder das Produkt kopieren kann, muss es andere Faktoren in den Mittelpunkt stellen (wie etwa Preis, Service, Support, Komfort, Qualität, Innovation etc.), um wettbewerbsfähig zu bleiben.

Dass ein Unternehmen die Anleitung öffentlich macht, heißt natürlich nicht, dass irgendjemand anderes Rechte daran hat. So wie Künstler und Autoren die legale Nutzung ihrer Werke an Bedingungen koppeln, werden auch die Entwickler oder Urheber eines Herstellungsverfahrens oder einer Anleitung Nutzungsbedingungen festlegen. Häufig ist die Nutzung nur für den privaten Gebrauch oder für Ausbildungszwecke gestattet. Man kann sich ansehen, was das Unternehmen geleistet hat, und dann sein eigenes Produkt entwickeln, man darf jedoch nicht einfach nur Kopien anfertigen und verkaufen. Die Nutzungsbedingungen für Open-Source-Software legen in der Regel fest, ob andere Unternehmen, die die Software modifizieren, zur Veröffentlichung ihrer Änderungen verpflichtet sind und ob sie die Software kommerziell verwenden dürfen.

Entwicklungsmodelle und Betriebssysteme für mobile Geräte

Das Entwicklungsmodell ist nur ein Aspekt von vielen, die die Philosophie und die Ziele eines Unternehmens widerspiegeln. Ein Unternehmen, das ein Open-Source-Betriebssystem für mobile Geräte wie Google Android entwickelt, hat nur geringen Einfluss darauf, wie es genutzt wird und wer es modifizieren kann. Ein Unternehmen, das ein Closed-Source-Betriebssystem wie Microsoft Windows entwickelt und an Gerätehersteller lizenziert, hat größeren Einfluss. Microsoft weiß, dass das Betriebssystem nicht modifiziert wird, und kann wählerisch sein, für welche Geräte es lizenziert wird. Ein Unternehmen, das ein Closed-Source-Betriebssystem wie Apple iOS für die eigenen Geräte entwickelt, kann Software entwickeln, die für die Hardware maßgeschneidert ist, auf der sie laufen soll. Dass ein Unternehmen, das ein Betriebssystem entwickelt, das von anderen nach Belieben modifiziert werden kann, und ein Unternehmen, das ein auf die eigene Hardware zugeschnittenes Betriebssystem entwickelt, völlig verschiedene Philosophien und Ziele verfolgen, liegt auf der Hand.

Man darf nicht außer Acht lassen, dass die Hersteller von Geräten für ein Open-Source-Betriebssystem wie Android keineswegs die gleiche Philosophie wie der Entwickler des Betriebssystems verfolgen müssen. Sie haben womöglich ganz andere Ziele und setzen auf ein anderes Entwicklungsmodell. Wenn die Lizenzbedingungen es erlauben, können die Gerätehersteller das Betriebssystem modifizieren, bevor sie es auf ihren Geräten installieren, ohne diese Änderungen jemals zu veröffentlichen.

Vielleicht ermöglichen die Änderungen lediglich das Funktionieren spezieller Hardware, die Hersteller können jedoch auch unerwünschte Apps installieren, die nicht löschbar sind und dazu führen, dass Apps von Drittherstellern nicht richtig funktionieren, weil sie die Änderungen nicht berücksichtigen, oder aber Informationen über die Nutzung des Geräts sammeln.

Zusammengefasst ist der entscheidende Punkt, dass ein Hersteller ein Open-Source-Betriebssystem auf einem Gerät einsetzen kann, das ansonsten Closed Source verwendet. Sie dürfen nicht glauben, dass ein Gerät an sich Open Source ist, nur weil das verwendete Betriebssystem Open Source ist. Tatsächlich können nur die wenigsten der Geräte mit einem Open-Source-Betriebssystem als echte Open-Source-Produkte betrachtet werden.

Wenden Sie die bereits beschriebene Vorgehensweise bei der Entwicklung eines Open-Source-Produkts auf Smartphones an. Die weitreichendste Interpretation eines Open-Source-Smartphones würde bedeuten, dass der Hersteller alle Informationen und sämtlichen Code veröffentlicht, die man braucht, um ein identisches Smartphone nebst aller eingesetzter Komponenten zu bauen. Wahrscheinlicher (wenngleich selten) ist es, dass die komplette Software (inklusive Betriebssystem, Treiber und Firmware), die bei der Auslieferung auf dem Gerät vorhanden ist, Open Source ist.

24.2.2 Apple iOS

Apples Closed-Source-Betriebssystem für mobile Geräte heißt *iOS* (Abbildung 24.15) und läuft auf dem iPhone, dem iPad und dem iPod touch. (Auf der Apple Watch läuft ein anderes Closed-Source-Betriebssystem namens WatchOS.) Apple kontrolliert die Entwicklung der Hardware, des Betriebssystems und der Entwicklerwerkzeuge sowie die Verfügbarkeit von Apps rigoros. Für Entwickler gelten strenge Vorschriften und Richtlinien – und das trägt dazu bei, dass iOS ein ziemlich sicheres System ist.



Abb. 24.15: iOS 13 auf dem iPhone

iOS-Apps sind fast ausschließlich über Apples *App Store* erhältlich. Eine Ausnahme stellen spezielle Apps dar, die größere Unternehmen ihren Mitarbeitern selbst zur Verfügung stellen können. Solche Apps werden innerhalb des Unternehmens entwickelt, können aber nur auf Geräten installiert werden, die unter der Kontrolle des fraglichen Unternehmens stehen und umgehen so den App Store. Dazu ist allerdings eine entsprechende Vereinbarung mit Apple erforderlich, in der die Vergabe von Unternehmenslizenzen geregelt wird.

24.2.3 Google Android

In gewisser Weise stellt *Android* eine Art Gegenpol zu iOS dar. Android ist eine Open-Source-Plattform, die ihrerseits auf einer Open-Source-Plattform beruht, nämlich auf Linux, und gehört Google (Abbildung 24.16). Open Source bedeutet, dass die Gerätehersteller Android nach ihrem Gutdünken ändern und anpassen können, daher gibt es Unterschiede zwischen den Versionen verschiedener Anbieter. Google stellt den grundlegenden Android-Code zur Verfügung und veröffentlicht hin und wieder neue Versionen (wobei die großen Updates nach einer Süßigkeit benannt werden). Die Hersteller passen den Code an besondere Funktionalitäten ihrer Hardware an und drücken ihm hinsichtlich der Bedienung und des Aussehens ihren eigenen Stempel auf.



Abb. 24.16: Android 8 (Oreo)

Apps sind in verschiedenen App-Stores wie Google Play oder dem Amazon App-Store verfügbar. Android-App-Stores sind ziemlich offen im Vergleich zu den hohen Standards, die Apple bei der strengen Kontrolle von App-Entwicklern verlangt. Android erleichtert es, beliebige von einer Website heruntergeladene Apps zu installieren.

Hinweis

Android-Geräte sind im Allgemeinen offener als iOS-Geräte, das muss aber nicht so sein. Wie offen oder restriktiv ein bestimmtes Android-Gerät ist, hängt in erster Linie davon ab, wie der Hersteller das Betriebssystem modifiziert hat.

24.2.4 Funktionalitäten der Betriebssysteme

Die Betriebssysteme mobiler Geräte unterscheiden sich voneinander und besitzen mitunter sowohl verschiedene Funktionalität als auch andere Bedienoberflächen. Sie haben aber auch sehr viel gemeinsam, denn der Benutzer erwartet natürlich, dass irgendein Gerät dieselben Aufgaben erledigen kann, von denen sie wissen, dass andere mobile Geräte sie erledigen können – unabhängig davon, ob Sie ein iPhone, ein Android-Smartphone oder eine Smartwatch benutzen. Sie erwarten, dass Sie Texte versenden, E-Mails abrufen und Videotelefonate führen können. Die Unterschiede zwischen den Betriebssystemen laufen letztlich darauf hinaus, dass sich die Hardware und die Apps unterscheiden, das »Look & Feel«, die typische Benutzererfahrung, und philosophische Unterschiede, die sich dadurch äußern, wie das Betriebssystem bestimmte Aufgaben in Angriff nimmt. Wir sehen uns kurz einige der Features an, die beide Betriebssysteme gemeinsam haben. Ich werde dabei auf die Unterschiede hinweisen.

Bedienoberflächen

Alle Betriebssysteme für mobile Geräte besitzen eine grafische Benutzeroberfläche, mit der Sie auf die Icons auf dem Bildschirm zugreifen können. Die aktuellen Modelle bieten keine Kommandozeile. Die verschiedenen Betriebssysteme verwenden entweder eine einzelne Haupttaste oder eine Iconleiste, um dem Benutzer den Zugang zu den wichtigsten Funktionen zugänglich zu machen. Außerdem kommen in allen Systemen Gesten wie z.B. Streichen zum seitenweisen Blättern oder das Auseinanderspreizen zweier Finger zum Zoomen zum Einsatz. Für gewöhnlich gibt es eine Art Menüsystem, das es dem Benutzer ermöglicht, zu bestimmten Apps oder Daten zu gelangen.

iOS erlaubt einige Anpassungen der Benutzeroberfläche. Sie können beispielsweise Apps gruppieren, indem Sie sie in Ordnern zusammenfassen oder Apps dort platzieren, wo Sie es möchten. Die Benutzererfahrung bleibt dennoch konsistent.

Android verwendet eine ganz andere Benutzeroberfläche, bei der sogenannten *Launcher* zum Einsatz kommen, also Software, die es dem Anwender erlaubt, sein System ausgiebig seinen Wünschen anzupassen. Es gibt Launcher von vielen verschiedenen Herstellern und die Hersteller liefern ihre Geräte mit den von ihnen bevorzugten Launchern aus. Die Geräte von Samsung verwenden beispielsweise *Touch Wiz*. Auf meinem Android-Smartphone benutze ich den Launcher Nova. Er erlaubt es, fast sämtliche Aspekte der Benutzeroberfläche umzugestalten, beispielsweise die Symbolgröße, Animationen, Gesten und mehr.

Die meisten mobilen Geräte besitzen einen Beschleunigungssensor und ein Gyroskop, um Bewegungen und die räumliche Orientierung feststellen zu können. Die Betriebssysteme nutzen diese Informationen, um in bestimmten Apps die Bildschirmausrichtung anzupassen. Wenn Sie beispielsweise ein Video betrachten möchten, können Sie das Gerät einfach von der Vertikalen in die Horizontale drehen, um eine bessere Anzeige zu bekommen. (Lesen Sie hierzu auch den Abschnitt 24.3.2, *Apps hinzufügen*, später in diesem Kapitel.)

WLAN-Telefonie

Natürlich muss ein Smartphone zum Telefonieren auf das Mobilfunknetz zugreifen können, Sie können aber auch über WLAN Telefongespräche oder Videotelefonate führen. WLAN-Telefonie erweist sich als besonders nützlich, wenn Sie sich des Öfteren in Umgebungen mit schlechter Mobilfunkabdeckung, aber gutem WLAN-Zugang aufhalten. Falls Sie die WLAN-Telefonie verwenden möchten, muss sowohl Ihr Smartphone als auch Ihr Mobilfunkanbieter das unterstützen. Zudem müssen Sie die

Funktion in den Einstellungen aktivieren (Abbildung 24.17). Nachdem das erledigt ist, kann Ihr Smartphone für alle Telefongespräche das WLAN verwenden, sofern eine ordentliche WLAN-Verbindung verfügbar ist.



Abb. 24.17: WLAN-Anrufe auf dem iPhone aktivieren

Virtuelle Assistenten

»Hey, Siri!«

»Ja, Mike?«

»Wie sieht es heute mit dem Wetter aus?«

»Wo du bist, scheint doch immer die Sonne, Mike.«

Nun ja, das ist vielleicht ein wenig übertrieben, aber tatsächlich gestatten es die virtuellen Assistenten der neuesten Smartphones und Tablets, häufig anfallende Tätigkeiten schnell und einfach durch sprachliche Interaktion zu erledigen. Sie brauchen beispielsweise *Siri*, Apples virtuelle Assistentin, nur nach einem nahegelegenen Restaurant oder einer Touristenattraktion zu fragen. Sie (die Stimme ist standardmäßig weiblich) antwortet dann mit den entsprechenden Informationen. Die virtuellen Assistenten helfen auch bei der Suche im Internet und können sogar bestimmte Apps auf dem Smartphone oder dem Tablet starten und verwenden. Für Leute mit einem Handicap, das es schwierig macht, den Touchscreen zu bedienen, ist das sehr hilfreich, weil sie Sprachbefehle verwenden können.

Ein virtueller Assistent kann auch beim Autofahren nützlich sein, wenn Sie während der Fahrt Ihr Smartphone verwenden müssen (wenngleich davon aus Sicherheitsgründen abzuraten ist). Bitten Sie den Assistenten darum, einen Anruf zu tätigen oder Ihnen Navigationsanweisungen vorzulesen, insbesondere wenn Ihr Smartphone mit dem Bluetooth-System des Fahrzeugs gekoppelt ist. Das Siri-Pendant in Windows 10 heißt *Cortana* und bietet im Wesentlichen die gleichen Funktionen und Dienste. Googles virtueller Assistent *Google Assistant* und steht nicht nur für Android, sondern auch für iOS und andere Google-Plattformen, wie Google Home oder Android TV, zur Verfügung. Neben diesen drei bekannten virtuellen Assistenten stehen, je nach Plattform, verschiedene andere Apps zum Herunterladen zur Verfügung, die weitere Dienste durch virtuelle Assistenten bereitstellen.

Software Development Kits

Zu jedem Betriebssystem für mobile Geräte gehört ein *SDK* (*Software Development Kit*), mit dem Sie eigene Anwendungen entwickeln oder vorhandene erweitern können. Abbildung 24.18 zeigt Xcode, die Entwicklungsumgebung für iOS, beim Testen einer App.

Jedes der Betriebssysteme stellt die Entwickler vor andere Herausforderungen. Apples strenge Regeln für Entwickler schreiben vor, dass jede App einem gründlichen Testprogramm unterzogen wird, bevor sie für den Vertrieb über den App Store zugelassen wird. Microsofts Modell für Entwickler funktioniert ähnlich, ist im Allgemeinen aber nicht ganz so streng. Google hingegen gestattet es jedem, Android-Apps zu entwickeln und zu vertreiben, ohne dabei auf besonders Weise einzugreifen.



Abb. 24.18: Xcode führt eine mit dem iOS-SDK entwickelte App aus.

Wichtig

Zum Programmieren von Apps wird ein *SDK* (*Software Development Kit*) verwendet. Verwechseln Sie es nicht mit dem *APK* (*Android Application Packet*), das den kompilierten Code einer App enthält und zur Installation dieser App auf einem Android-Gerät dient.

Mobile Bezahldienste

Smartphones und andere mobile Geräte sind inzwischen im Alltag derart allgegenwärtig, dass wir auf ihnen auch persönliche oder sensible Daten speichern, wie beispielsweise Kennwörter, Kontoauszüge, Kreditkarteninformationen oder Zugangsdaten für das Onlinebanking. Im Laufe der Zeit haben Smartphone-Hersteller und Händler erkannt, dass es der nächste logische Schritt dieser Entwicklung wäre, es zu ermöglichen, mit dem Smartphone für Güter und Dienstleistungen zu bezahlen, indem man einfach die dazu erforderlichen Daten ausliest oder eine App zum Bezahlen verwendet.

Die App hätte Zugriff auf Ihre Kontodaten und würde automatisch die Zahlung an den jeweiligen Händler veranlassen. Das Ganze wird dann als *mobiler Bezahldienst* bezeichnet. Oftmals benötigen Sie noch nicht einmal eine App, denn viele Händler nutzen NFC-Anwendungen (*Near Field Communication*), die vom Smartphone eine Zahlungsfreigabe erhalten, indem es einfach kurz auf oder neben einer speziellen Ablage an der Kasse platziert wird. (Mehr zu diesem Thema im Abschnitt *NFC*.)

Darüber hinaus haben die Smartphone-Hersteller ihre eigenen Bezahlsysteme entwickelt. So hat Apple beispielsweise kürzlich einen Bezahldienst namens *Apple Pay* vorgestellt. Apple Pay wurde erstmals im iPhone 6 implementiert und sogar die Apple Watch unterstützt dieses Bezahlsystem. In den

USA kann an allen Terminals der bekannten Kreditkartenunternehmen wie Visa, MasterCard oder American Express, die bei der Entwicklung des Systems einbezogen wurden, mit Apple Pay bezahlt werden. Mit Apple Pay kann an NFC-Terminals berührungslos bezahlt werden und bei online erworbenen Apps werden In-App-Käufe unterstützt.

Flugmodus

Der *Flugmodus* ist ein einfacher Schalter (entweder ein echter, mechanischer Schalter am Gerät oder ein Software-Schalter, der in den Systemeinstellungen des Geräts zu finden ist), der alle drahtlosen Dienste (Mobilfunk, WLAN, Bluetooth) des Geräts gleichzeitig abschaltet (Abbildung 24.19). Dadurch ist gewährleistet, dass keine Signale gesendet oder empfangen werden können. Der Flugmodus wird vor allem dann benutzt, wenn die Passagiere eines Flugzeugs dazu aufgefordert werden, ihre mobilen Geräte abzuschalten – daher auch der Name. Sie können den Flugmodus aber auch verwenden, um alle Kommunikationsfunktionen schnell zu deaktivieren.

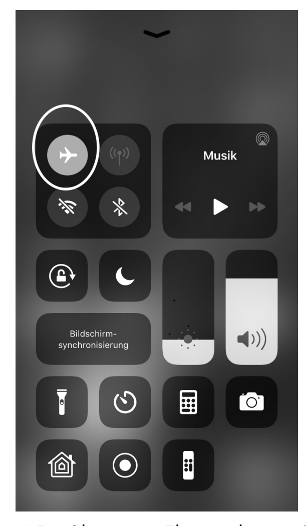


Abb. 24.19: Aktivierter Flugmodus in iOS 13

Firmware für Funkverbindungen

Mobile Geräte nutzen verschiedene Funktechnologien, um auf das Internet, E-Mail und die Infrastrukturen von Unternehmen zuzugreifen. Im Allgemeinen gibt es zwei Funkverbindungen: 802.11 und Bluetooth. Wenn man mit dem Gerät normale Anrufe tätigen kann, gibt es darüber hinaus noch Mobilfunk.

PRL-, PRI- und Baseband-Updates Wenn Sie auf Reisen sind, kommt es immer wieder vor, dass Sie Gebiete durchqueren, in denen die Signale zu schwach sind oder in denen Ihr Internetanbieter gar nicht präsent ist. Wenn sich ein Gerät mit verschiedenen Internetanbietern verbinden kann, nennt man das *Roaming* – und das kann mit zusätzlichen Kosten verbunden sein, je nachdem, um welchen Anbieter es sich handelt. Die *PRL* (*Preferred Roaming List*, die Liste der bevorzugten Anbieter beim Roaming) wird gelegentlich von Ihrem Anbieter automatisch in der Firmware aktualisiert, damit Ihr Gerät mit den Frequenzen der verschiedenen Anbieter in der bevorzugten Reihenfolge konfiguriert ist, wenn es keine Verbindung zum Netzwerk Ihres Internetanbieter herstellen kann.

Aktualisierungen dieser Liste werden über die Mobilfunkverbindung des Geräts übermittelt (man spricht dann von einem *Baseband*- oder *Over-the-air-Update*). Manchmal finden solche Aktualisierung auch im Rahmen einer »normalen« Aktualisierungen von Betriebssystem und Firmware statt, die bei einer Synchronisierung durchgeführt werden.

Bei CDMA-Geräten gibt es sogenannte *PRI*-Updates (*Product Release Information*). Sie steuern die Datenübertragungsrate zwischen mobilem Gerät und dem Funkmast und werden übermittelt, um zu gewährleisten, dass das mobile Gerät die Daten mit einer Datenrate sendet, mit der das Netzwerk des Anbieters sie empfangen kann.

Wichtig

PRL- und PRI-Updates werden bei der Aktualisierung des Betriebssystems oder der Firmware automatisch gehandhabt. Sie betreffen nur CDMA-Netzwerke. Nur die größten Freaks werden solche Updates jemals zu sehen bekommen.

IMEI, ICCID und IMSI Hierbei handelt es sich um drei IDs, die Sie nicht nur für die Prüfung kennen sollten, sondern auch bei der Verwaltung von mobilen Geräten in der Praxis benötigen. Die IMEI (*International Mobile Equipment Identity*) ist eine 15-stellige Nummer, die zur Identifizierung eines mobilen Geräts dient, typischerweise ein Smartphone oder ein anderes Gerät, das sich mit dem Mobilfunknetz verbindet. IMEIs sind innerhalb der GSM-Gerätefamilie (*Global System for Mobile Communications*) und deren Nachfolgetechnologien (das heutige 4G-LTE und LTE-Advanced) eindeutig. Typischerweise findet sich im Batteriefach des Geräts ein Aufkleber mit der IMEI, aber Sie müssen das Gerät oft gar nicht auseinandernehmen, denn das Betriebssystem kann sie meist in den Systemeinstellungen anzeigen (Abbildung 24.20).

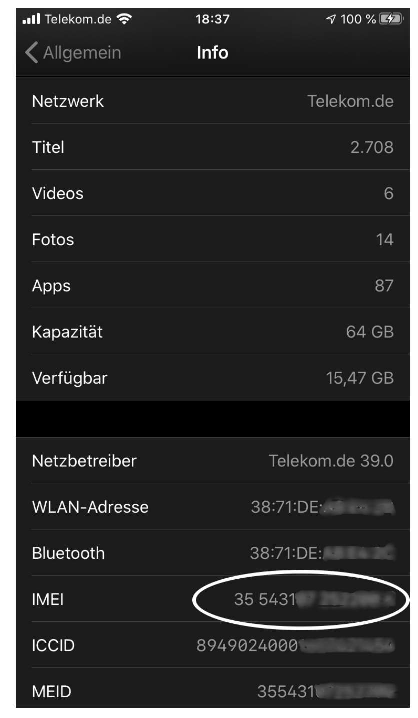


Abb. 24.20: Anzeige der IMEI

Die IMEI kann dazu verwendet werden, ein bestimmtes Gerät eindeutig zu identifizieren oder sogar, um dem Gerät den Zugang zum Netzwerk eines Anbieters zu verweigern. Wenn ein Gerät verloren geht oder gestohlen wird, kann der Eigentümer seinen Internetanbieter darüber informieren, der dann dafür sorgt, dass das fragliche Gerät das Netzwerk nicht nutzen darf.

Tipp

Notieren Sie sich immer die IMEI neuer Smartphones, denn anhand dieser Nummer können Sie nachweisen, dass Sie der rechtmäßige Eigentümer sind, falls das Gerät verloren geht oder gestohlen wird.

Die *ICCID* (*Integrated Circuit Card Identifier*) ist die eindeutige Kennung einer SIM-Karte (*Subscriber Identy Module*). Die SIM-Karte enthält Informationen über den Eigentümer des Smartphones und dient dazu, den Benutzer gegenüber dem Netzwerk zu identifizieren. SIM-Karten können für gewöhnlich problemlos von verschiedenen Mobiltelefonen genutzt werden.

Die dritte Zahl namens *IMSI* (*International Mobile Subscriber Identity*) ist ebenfalls auf der SIM-Karte gespeichert und repräsentiert den der SIM-Karte zugeordneten Benutzer. Auf diese Nummer kann das Mobiltelefon normalerweise nicht zugreifen, sie kann jedoch beim Anbieter erfragt werden, um sicherzustellen, dass gestohlene Geräte nicht missbraucht werden. Die IMSI-Nummer kann auch zum Freischalten eines Geräts verwendet werden. Unter Umständen kann es sinnvoll sein, die Nummern aller Geräte eines Unternehmens zwecks Inventarisierung oder zur Verwendung in der MDM-Software (*Mobile Device Management*) zu notieren. Bei der Vergabe der Geräte werden typischerweise diese Nummer sowie andere eindeutige Merkmale eines Geräts erfasst, wie z.B. Telefonnummer oder MAC-Adresse, und im Verzeichnis aller mobilen Geräte gespeichert. Abbildung 24.21 zeigt IMEI und ICCID in den Systemeinstellungen eines neueren Android-Geräts.

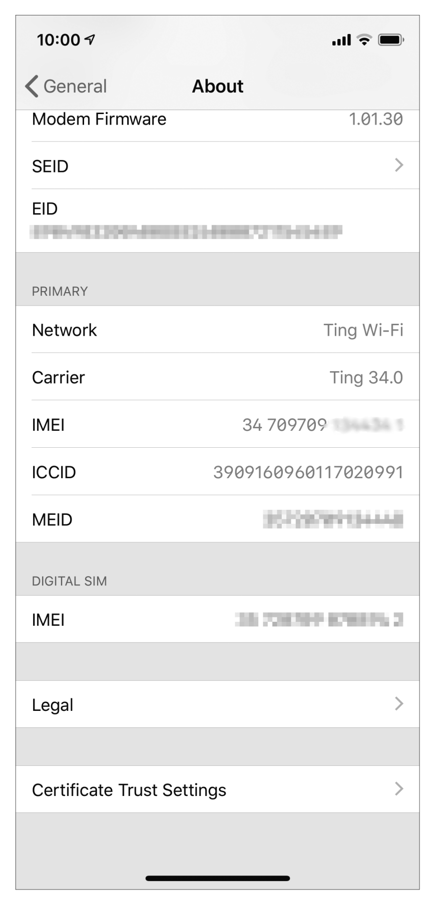


Abb. 24.21: IMEI und ICCID-Nummer

Wichtig

Merken Sie sich für die CompTIA A+-Prüfung den Unterschied zwischen IMEI und IMSI. Die IMEI repräsentiert das Gerät, die IMSI hingegen identifiziert das Benutzerkonto beim Anbieter und ist auf der SIM-Karte gespeichert.

VPN

Wie Sie aus den vorhergehenden Kapiteln wissen, ermöglichen VPNs eine sichere Verbindung zwischen einem Client und der Infrastruktur eines Unternehmens oder zwischen zwei entfernten Netzwerken, z.B. zwischen der Zentrale eines Unternehmens und einer Filiale. Typischerweise verwenden VPNs einen Tunnel durch unsichere Netzwerke wie das Internet. Auf einem VPN-Client läuft eine spezielle Software, die für die Verbindung zum VPN-Server des Firmennetzwerks konfiguriert sein muss. Die Konfiguration umfasst die Verschlüsselungsmethode sowie das Authentifizierungsverfahren, wie beispielsweise eine Kombination aus Benutzernamen und Kennwort oder ein digitales Zertifikat.

Bei einer VPN-Verbindung zweier Netzwerke kommen auf beiden Seiten VPN-Server zum Einsatz, die so konfiguriert sind, dass sie über eine verschlüsselte Verbindung miteinander kommunizieren können. Die Hosts in den beiden Netzwerken nutzen den jeweiligen VPN-Server als Gateway. Die Benutzer bekommen davon für gewöhnlich nichts mit – für sie sieht es so aus, als ob die Hosts des anderen Netzwerks direkt mit ihrem eigenen Netzwerk verbunden wären.

Zur Einrichtung eines VPNs steht eine Vielzahl von Technologien und Protokollen zur Verfügung. Am verbreitetsten sind eine Kombination aus L2TP (*Layer 2 Tunneling Protocol*) und IPsec (Abbildung 24.22) sowie SSL/TLS (*Secure Socket Layer/Transport Layer Security*). Das L2TP/IPsec-Verfahren nutzt den UDP-Port 1701, der auf beiden Seiten der Verbindung geöffnet sein muss.

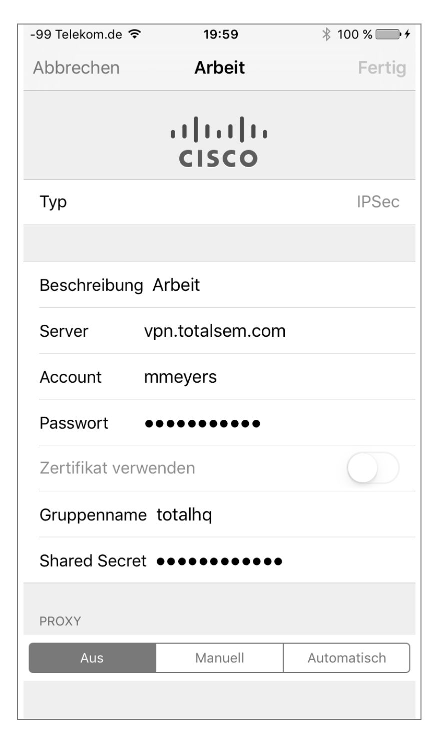


Abb. 24.22: Konfiguration eines VPNs

Bei einem nach diesem Muster aufgebauten VPN verbinden sich die Benutzer mit dem Firmennetzwerk und können ihre Anwendungen (E-Mail-Client, Dateifreigaben usw.) so benutzen, als ob sie vor Ort mit dem Firmennetzwerk verbunden wären.

Ein SSL/TLS-basiertes VPN hingegen verwendet den SSL/TLS-Standardport TCP 443 und wird typischerweise über einen Webbrowser genutzt. Auf dem Client selbst ist dafür normalerweise keine spezielle Software oder Konfiguration erforderlich. Allerdings ist die Funktionalität eines SSL/TLS-basierten VPNs oftmals etwas eingeschränkt, wenn auf die Unternehmensressourcen in Form eines Zugangsportals über einen Webbrowser zugegriffen werden muss.

24.3 Konfiguration

Damit Smartphone und Tablet tadellos im Netzwerk funktionieren, müssen einige Dinge eingerichtet und konfiguriert werden. Moderne Geräte sind typischerweise vorkonfiguriert und Sie müssen nur noch ein Benutzerkonto und Zugangsdaten angeben, damit ist die Einrichtung aber noch nicht erledigt.

Sie können die Fähigkeiten des Geräts durch zusätzlich Hardware erweitern und Apps zur Steigerung der Produktivität installieren. Sie müssen außerdem die Netzwerkverbindung konfigurieren, Bluetooth-Geräte hinzufügen, sowie E-Mail-Zugänge und die Synchronisierung mit dem PC einrichten. Darüber hinaus stehen viele weitere Optionen zur Verfügung. Sehen wir uns das näher an.

24.3.1 Erweitern der Hardware

Mobile Geräte sind Computer wie Desktop-PCs, besitzen prinzipiell die gleichen Komponenten und können ähnliche Aufgaben erledigen. Auf der Hauptplatine des Geräts, dem Mainboard, sind die übrigen Bauteile angebracht. Das größte dieser Bauteile ist oft das sogenannte *SoC* (*System on a Chip*). Dieses Wunder der Miniaturisierung vereint CPU, GPU und allerlei weitere Logikbausteine auf einem einzigen Siliziumchip, wodurch viel Platz und Energie eingespart wird. Interessanterweise kommen hier kaum Intel-x86-basierte Chips zum Einsatz. Viel wahrscheinlicher ist es, eine ARM-Architektur vorzufinden, wenn Sie die Spezifikationen Ihres neuen Tablets studieren. Beispielsweise verwendet das iPad einen von Apple entworfenen ARM-Chip der A-Reihe und das ASUS Transformer ein von NVIDIA entwickeltes Tegra-ARM-SoC.

Als Massenspeicher werden keine herkömmlichen magnetischen Festplatten (HDDs), sondern *SSDs* (*Solid-State-Drives*) und microSD-Karten eingesetzt, weil diese kleiner, energiesparender und viel schneller als rotierende HDDs sind. Außerdem erzeugen sie weniger Wärme.

Mobile Geräte unterscheiden sich von ihren größeren Verwandten in zwei Bereichen, die für Techniker von großer Bedeutung sind. Zum einen gibt es keine austauschbaren Ersatzteile. Wenn etwas kaputtgeht, müssen Sie das Gerät zum Hersteller senden, einen örtlichen autorisierten Händler aufsuchen, wie z.B. einen Apple Store, oder es zu einer darauf spezialisierten Reparaturwerkstatt bringen. Zum anderen lassen sich die Geräte nicht aufrüsten. Selbst bei Laptops lässt sich zumeist der Arbeitsspeicher erweitern oder die Festplatte austauschen, aber bei mobilen Geräten müssen Sie sich mit dem zufriedengeben, was Sie gekauft haben. Wenn Sie etwas Besseres haben möchten, müssen Sie ein neues Gerät erwerben.

Nachdem das geklärt ist: Sie können an mobilen Geräten verschiedene externe Peripherie- oder Speichergeräte anschließen. In dieser Hinsicht unterscheiden sich die verschiedenen Modelle aber sehr, daher ist es schwierig, hier zu verallgemeinern.

Wie so oft gibt es eine Ausnahme von der Regel, keine allgemeinen Aussagen über mobile Geräte zu treffen, und diese betrifft den Sound. Noch besitzen die meisten Geräte einen 3,5-mm-Klinkenstecker zum Anschluss von Kopfhörern oder Lautsprechern (Abbildung 24.23). Das ändert sich allerdings gerade, denn Apple hat den Anschluss mit dem iPhone 7 abgeschafft, und bei vielen hochwertigen Android-Geräten fehlt er jetzt auch. Aktuelle iPhones und iPads verwenden stattdessen nun den Lightning-Anschluss.



Abb. 24.23: Smartphone mit angeschlossenem Kopfhörer

Erweiterungsmöglichkeiten bei Apple-Geräten

Apples Geräte bieten die geringsten Erweiterungsmöglichkeiten. Auch wenn sie in den USA marktbeherrschend sind, gibt es daher hier nicht viel zu sagen. Die meisten Erweiterungsmöglichkeiten sind auf proprietäre Kabel und Geräte beschränkt. iPhone und iPod verwenden einen einzigen proprietären Anschluss, der zum Aufladen des Geräts und zum Anschluss der verfügbaren externen Geräte dient. Abbildung 24.24 zeigt die typische Verwendung des Anschlusses mit einem per USB-Kabel angeschlossenen Ladegerät.



Abb. 24.24: Am iPad angeschlossenes Ladegerät

Die meisten iOS-Geräte verwenden den proprietären Lightning-Anschluss, aber mit den aktuellen iPad Pros hat Apple USB Typ C eingeführt. Was das für kommende iPhones bedeutet, ist unklar, aber es ist erfreulich, dass Apple die Nutzung des Industriestandards ausdehnt. Ich komme später bei der Betrachtung einer Reihe von Steckern auf USB Typ C zurück.

iPhones und iPads können Bildschirminhalte auf externen Geräten ausgeben, wie z.B. auf einem Projektor. Dadurch ist es auf einfachste Weise möglich, beispielsweise mit Apples exzellentem Präsentationsprogramm *Keynote* Vorträge zu halten (Abbildung 24.25). Für die Verbindung ist ein Adapter erforderlich (Abbildung 24.26).



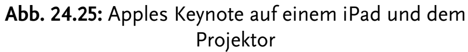

Abb. 24.25: Apples Keynote auf einem iPad und dem Projektor



Abb. 24.26: Apples digitaler A/V-Adapter

Erweiterungsmöglichkeiten bei Android-Geräten

Die Geräte, die mit Google Android ausgeliefert werden, besitzen eine Reihe verschiedener Anschlüsse und Erweiterungsmöglichkeiten. Viele verfügen über einen MicroSD-Steckplatz, um Speicherkapazität in Form kleiner Flash-Speicherkarten hinzuzufügen (Abbildung 24.27).



Abb. 24.27: MicroSD-Karte und Steckplatz

Die meisten Android-Geräte verwenden zum Laden und Anschließen von Erweiterungen Standard-USB-C- oder Micro-USB-Anschlüsse, manche Geräte bieten auch Mini-USB oder sogar einen USB-Anschluss normaler Größe. Einige ältere Android-Geräte besitzen zu diesem einen proprietären Anschluss (der meist ebenfalls auf USB-Technologie beruht), aber dabei handelt es sich fast ausnahmslos um Tablets. Abbildung 24.28 zeigt einen solchen proprietären Stecker.



Abb. 24.28: Proprietärer ASUS-Stromanschluss

Schließlich besitzen viele Tablets einen Anschluss für einen externen Monitor oder einen Projektor. (Smartphones besitzen einen solchen Anschluss im Allgemeinen nicht.) Abbildung 24.29 zeigt einen Micro-HDMI-Anschluss nebst passendem Stecker.



Abb. 24.29: Micro-HDMI-Anschluss und -Stecker

Bluetooth

Auch auf drahtlosem Weg lassen sich mobile Geräte erweitern. Zum Anschluss von Tastaturen, Headsets, Mäusen (nicht bei Apple-Geräten) oder Lautsprechern wird vornehmlich Bluetooth (siehe Kapitel 20) verwendet. In Abbildung 24.30 sehen Sie die kleine Apple-Tastatur fürs iPad, das in einer Halterung steht, um das Tippen etwas einfacher als mit der virtuellen Tastatur zu gestalten. Bluetooth-fähige Wearables erfreuen sich zunehmender Beliebtheit, und manchmal kann es schwierig sein, zu entscheiden, wie eigenständig diese Geräte sein dürfen, um noch als Erweiterung zu gelten und nicht als vollwertiges Gerät.



Abb. 24.30: Bluetooth-Tastatur für das iPad

> **Hinweis**
>
> Im Abschnitt *Bluetooth* am Ende dieses Kapitels wird die Einrichtung einer Bluetooth-Tastatur bei einem Tablet ausführlich beschrieben.

24.3.2 Apps hinzufügen

Die Geräte werden von den Herstellern mit einer gewissen Anzahl unverzichtbarer Apps ausgeliefert (E-Mail, Browser, Notizen, Kalender usw.). Darüber hinaus bringen die meisten Geräte auch Multimedia-Apps zur Musikwiedergabe, zum Fotografieren, zum Abspielen von Videos und zur Anzeige von Fotos mit. Es gibt auch verschiedene Werkzeuge für Kurznachrichtendienste und im Fall von Smartphones natürlich Telefonieanwendungen.

Zur Installation der meisten anderen Apps wird ein App-Store verwendet. Beachten Sie, inwieweit die Ökosysteme der Apps für die Betriebssysteme der mobilen Geräte zu den am Anfang dieses Kapitels erörterten Entwicklungsmodellen passen. Für gewöhnlich spiegeln die Regeln des Ökosystems das Entwicklungsmodell wider, Sie dürfen aber nicht glauben, dass sich alle angebotenen Apps daran halten. Es gibt jede Menge Closed-Source-Apps für Android und Open-Source-Apps für iOS.

iOS-Apps

Auf iPhones und. iPads läuft das Betriebssystem iOS bzw. iPadOS. Anders als die anderen Hersteller versucht Apple, die Benutzererfahrung streng zu kontrollieren, und besteht darauf, dass alle iOS-Entwickler bestimmten Regeln folgen müssen.

Apple kontrolliert daher strikt, welche Apps auf iOS-Geräten installiert werden können, und das bedeutet, dass Sie Apps für das iPhone oder das iPad nur im Apple App Store (Abbildung 24.31) erhalten. Apple prüft alle Apps vor der Veröffentlichung im App Store und behält sich das Recht vor, Apps zu entfernen, die sich nicht an die Regeln halten.



Abb. 24.31: App Store

Wählen Sie auf dem Startbildschirm das App-Store-Symbol aus, um eine App zu installieren. Sie können auf der Registerkarte HEUTE aus den Highlights auswählen oder sich verschiedene Kategorien anzeigen lassen. Sehen Sie sich die beliebtesten Spiele an oder suchen Sie einfach nach dem, was Sie sich wünschen (Abbildung 24.32).

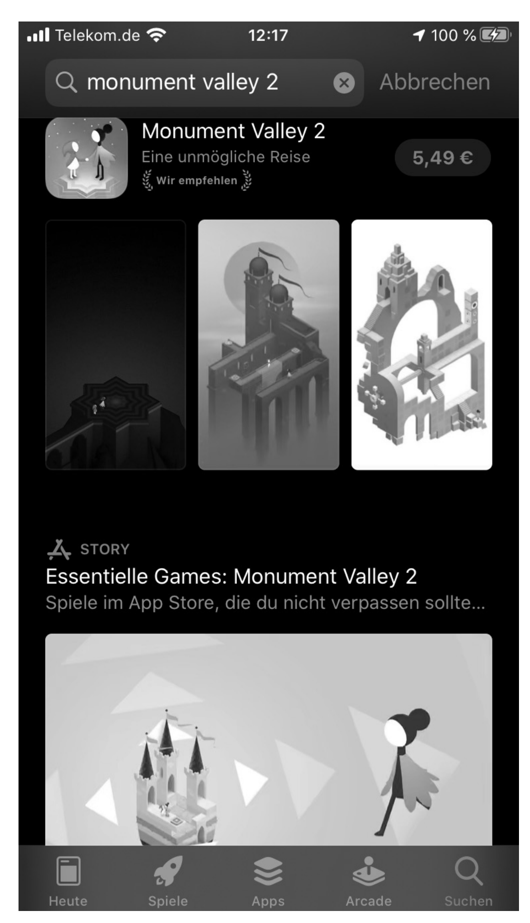


Abb. 24.32: Suche nach Monument Valley 2

Wenn Sie zum ersten Mal eine App im App Store kaufen, werden Sie zur Einrichtung eines Benutzerkontos aufgefordert. Falls Sie bereits über ein Konto verfügen, das Sie beim Einkaufen im iTunes Store eingerichtet haben, können Sie dieses verwenden. Ansonsten richten Sie über den Apple-iCloud-Dienst ein neues Konto ein. Die Einrichtung erfordert einige Schritte und eine gültige Kreditkarte (Abbildung 24.33), aber das ist schnell erledigt.

Der iCloud-Schlüsselbund verwendet die Schlüsselbundverwaltung von macOS, um Benutzerdaten, Passwörter und andere Zugangsdaten verschlüsselt mit Ihren anderen Apple-Geräten zu synchronisieren. (Siehe nachfolgenden Abschnitt 24.3.6, *Synchronisierung*.) Der Schlüsselbund kann auch Zugangsdaten speichern, die nicht zu Apple gehören, wie etwa diejenigen von Facebook, Amazon oder anderen Diensten, und diese verwenden, um Formulare in Apps oder auf Websites automatisch auszufüllen. Der eigentliche Vorteil besteht darin, dass Sie Apple autorisieren können, diese sensiblen Daten zu speichern, anstatt jeder einzelnen App oder Website das Speichern zu gestatten.



Abb. 24.33: Einrichten einer Apple-ID

Android-Apps

Auf den meisten Smartphones und einem respektablen Anteil der Tablets läuft Googles Android. Android unterscheidet sich deutlich von Apples iOS, denn Google stellt das Betriebssystem kostenlos bereit und die verschiedenen Hersteller passen Android an ihre Geräte an. Mit anderen Worten: Auf einem Samsung-Tablet läuft ein etwas anderes Betriebssystem als auf einem ASUS-Tablet. OnePlus wiederum verwendet eine eigene Benutzeroberfläche namens OxygenOS Sense für die eigenen Android-Geräte, die das Aussehen und die Bedienung des Betriebssystems modifizieren.

Aufgrund dieser Änderungen verwenden nur die wenigsten Android-Benutzer ein unmodifiziertes Android. Trotz der gemeinsamen Teile des Betriebssystems sind Benutzer, die mit den Geräten eines Herstellers vertraut sind, manchmal von der verschiedenartigen Bedienoberfläche der Geräte eines anderen Herstellers verwirrt. Wegen dieser Unterschiede ist es wichtig, nicht nur die auf einem Smartphone oder Tablet laufende Android-Version zu kennen, sondern auch den Hersteller und dessen Modifikationen an Android. Üblicherweise vergeben die Hersteller eine Versionsnummer bei der Veröffentlichung der von ihnen vorgenommenen Änderungen.

Wenn Sie auf einem Android-Gerät eine App installieren möchten, stehen verschiedene Quellen dafür zur Verfügung. Am gebräuchlichsten ist der voreingestellte App-Store, Google Play (der mehr als 2 Millionen Apps anbietet), aber manche Hersteller, wie etwa Amazon mit der Fire-Produktreihe, ändern diese Einstellung. Viele Hersteller bieten an ihre Geräte angepasste Apps selbst an. Diese herstellerspezifischen Stores ermöglichen es Ihnen, Apps zu installieren, die auf Ihrem Android-Smartphone oder -Tablet ordentlich funktionieren.

Es gibt auch einige App-Stores von Drittanbietern mit Apps, die »für Android« entwickelt wurden und möglicherweise auf Ihrem Gerät funktionieren, aber eine Garantie, dass solche Apps auf allen Android-Geräten laufen, gibt es nicht. Diese Wild-West-Verhältnisse lassen die Android-Benutzererfahrung hinsichtlich Smartphones und Tablets gegenüber der iOS-Benutzererfahrung in einem anderen Licht erscheinen.

24.3.3 Netzwerkverbindung

Die Verbindung zur Außenwelt wird entweder über das Mobilfunknetz oder mittels einem der 802.11-Wi-Fi-Standards hergestellt. Diese Standards sind Ihnen aus Kapitel 20 bereits bekannt. Wir betrachten hier die Besonderheiten der Standardkonfiguration hinsichtlich mobiler Geräte.

Wenn Sie sich erstmals mit einem WLAN verbinden möchten, müssen Sie zunächst WLAN aktivieren und dann die Verbindung aufbauen. Wenn das drahtlose Netzwerk ordnungsgemäß für den Betrieb mit WPA, WPA2 oder WPA3 konfiguriert ist, müssen Sie darüber hinaus im Besitz der Zugangsdaten sein, um auf das Netzwerk zuzugreifen. Der übliche Weg zum Aufbau einer Verbindung führt über die App EINSTELLUNGEN (Abbildung 24.34).



Abb. 24.34: Auswahl der App EINSTELLUNGEN

Mit der App EINSTELLUNGEN können Sie fast alle erforderlichen Konfigurationen vornehmen. Wenn Sie sich mit einem Netzwerk verbinden möchten, tippen Sie auf WLAN (oder auf NETZWERKE), um die verfügbaren Netzwerke anzuzeigen (Abbildung 24.35). Wählen Sie das gewünschte Netzwerk aus und geben Sie das Kennwort ein. Haben Sie einen Moment Geduld, bis dem Gerät vom DHCP-Server eine IP-Adresse zugewiesen und DNS-Informationen übermittelt worden sind. Schon sind Sie mit dem Netzwerk verbunden.

Wenn Sie sich erfolgreich mit einem Netzwerk verbunden haben, merkt sich Ihr Gerät die Zugangsdaten automatisch und legt anhand der SSID (dem Namen des Netzwerks) ein *Netzwerkprofil* an. Das Ganze funktioniert auf die gleiche Weise wie bei allen anderen Geräten, die sich mit einem WLAN verbinden. Wenn die SSID des Netzwerks geändert wird, nachdem Sie sich verbunden haben, wird Ihr Gerät beim nächsten Versuch, sich mit dem umgetauften Netzwerk zu verbinden, scheitern. Sie müssen in diesem Fall das Netzwerkprofil löschen und sich erneut verbinden. Wählen Sie dazu in der App EINSTELLUNGEN das fragliche Netzwerk aus und tippen Sie auf DIESES NETZWERK IGNORIEREN.

Wichtig

Sie können die App EINSTELLUNGEN dazu verwenden, um WLAN abzuschalten oder um den FLUGMODUS zu aktivieren, sodass Ihr Gerät gar keine Signale mehr aussendet.

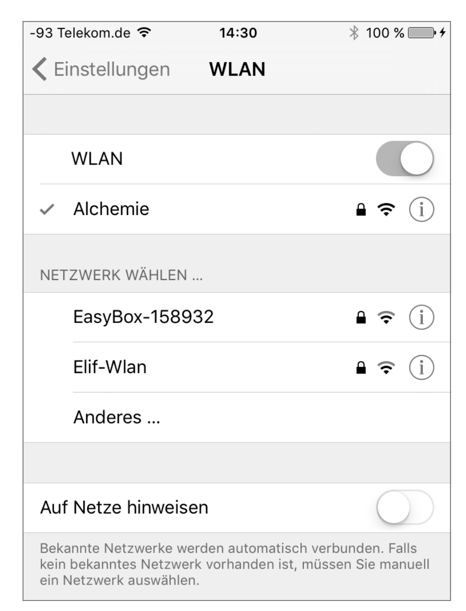


Abb. 24.35: Anzeige der verfügbaren Netzwerke

24.3.4 Daten

Viele mobile Geräte können die in Kapitel 20 beschriebenen Datendienste verwenden, um auf das Internet zuzugreifen. Sie können Ihr Gerät auf diese Weise fast überall zum Empfang von E-Mail oder zum Surfen im Internet verwenden.

Üblicherweise verwenden die mit Mobilfunknetzwerken verbundenen Smartphones oder Tablets das sogenannte *Roaming*, bei dem automatisch die Funkzelle oder der Netzwerkbetreiber gewechselt wird, ohne dass Sie etwas davon bemerken. Das ist keine große Sache, sofern Sie sich innerhalb der Landesgrenzen bewegen, wo die miteinander konkurrierenden Netzwerkbetreiber günstige Roaming-Verträge ausgehandelt haben.

Aber wehe, Sie bewegen sich in der Nähe der Landesgrenze oder gar außerhalb! Ihr mobiles Gerät wird sich mit Freuden in Mobilfunknetzwerke anderer Netzwerkbetreiber einbuchen, was zu horrenden Gebühren führen kann. Wenn Sie das von Ihrem Netzwerkbetreiber abgedeckte Gebiet öfter verlassen müssen, sollten Sie sich nach einem Mobilvertrag umsehen, der solche Ausflüge berücksichtigt. Zwar sind solche Verträge teurer als normale, die Preise sind aber nicht annähernd so exorbitant hoch wie bei einem unbeabsichtigten Roaming.

Wenn Sie im Grenzgebiet oder im Ausland auf die Internetverbindung verzichten können, sollten Sie das Roaming abschalten. Wie Sie wohl vermutet haben, können Sie das in der App EINSTELLUNGEN erledigen. Sie können die Datenverbindung auch komplett abschalten oder, sofern Ihr Gerät mehrere Dienste unterstützt, nur bestimmte erlauben. Wenn Ihr Vertrag beispielsweise keine unbegrenzten Datenverbindungen erlaubt und sich die bereits übertragene Datenmenge der vertraglichen Grenze nähert, wäre es sinnvoll, die Datenverbindung abzuschalten. Es kann auch aus Sicherheitsgründen sinnvoll sein, auf Reisen Mobilfunkverbindungen zu deaktivieren. . Ich komme in Kapitel 25 darauf zurück.

Wichtig

Die CompTIA nennt in den Lernzielen Google/Inbox als E-Mail-Programm. Wenn Sie diese Zeilen lesen, ist der Dienst in Gmail aufgegangen. Es könnte sein, dass in der Prüfung eine Frage Google/Inbox als richtige Antwort enthält.

24.3.5 E-Mail

Alle mobilen Geräte sind für den Empfang und Versand von E-Mail über den Dienst des jeweiligen Betriebssystemherstellers vorbereitet. Darüber hinaus können Sie das Gerät auch für den Zugriff auf andere Mailserver konfigurieren.

iOS, Android und Windows Phone bieten die E-Mail-Dienste von Apple, Google bzw. Microsoft an. Bei iOS-Geräten sind die iCloud-Dienste wie E-Mail, Nachrichten und iCloud Drive perfekt in das System integriert. Android-Geräte gehen davon aus, dass ein Gmail-Benutzerkonto verwendet wird, und sind für ein solches Konto vorbereitet. Windows-Geräte sind für die Nutzung von Exchange-Konten vorkonfiguriert. Die CompTIA hat für diese Art der automatischen Konfiguration einen ellenlangen Begriff parat: *integrierte E-Mail-Konfiguration durch kommerzielle Anbieter*. Aha!

Neben den integrierten E-Mail-Optionen kann auch der Zugriff auf andere Mailserver eingerichtet werden. Der Vorgang ähnelt dem in Kapitel 21 beschriebenen. Bei Apple-Geräten verwenden Sie dazu wieder die EINSTELLUNGEN. Wählen Sie dort PASSWÖRTER & ACCOUNTS (vor iOS 12: MAIL, KONTAKTE, KALENDER) aus (Abbildung 24.36). Tippen Sie nun ACCOUNT HINZUFÜGEN an, um die zur Verfügung stehenden E-Mail-Dienste anzuzeigen (Abbildung 24.37). Wenn Sie sich mit einem Microsoft Exchange-Server verbinden möchten, wählen Sie die entsprechende Option aus und geben Sie E-Mail-Adresse, Domain, Benutzername, Kennwort und Beschreibung ein.

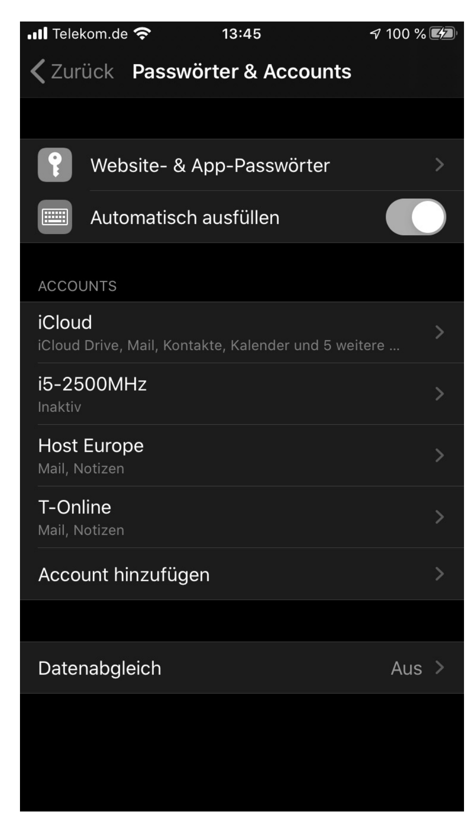


Abb. 24.36: Der Bildschirm PASSWÖRTER & ACCOUNTS auf einem iPhone

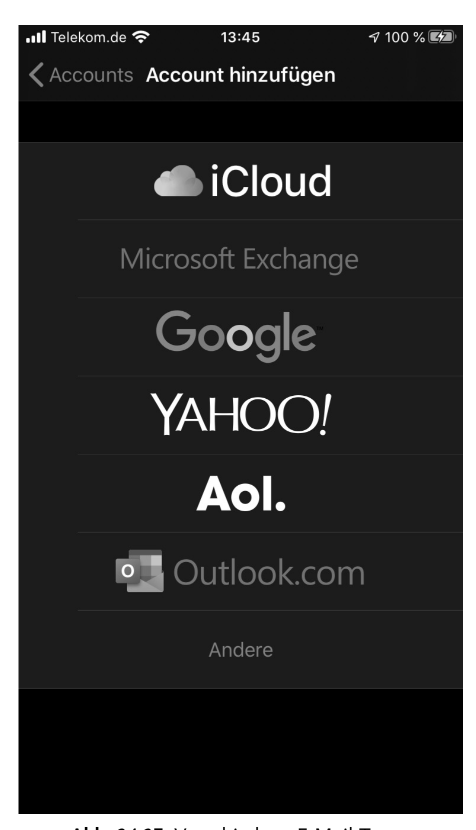


Abb. 24.37: Verschiedene E-Mail-Typen

Die gebräuchlichen POP3- oder IMAP4-Accounts gehören nicht zum Standardrepertoire, daher müssen Sie gegebenenfalls die Option ANDERE auswählen. Hier gelangen Sie schließlich zur Auswahl zwi-

schen POP3- und IMAP-Server und zur Aufforderung, die Adressen für die Server zum Versenden (SMTP) und Empfangen von E-Mail anzugeben.

Bei Android-Geräten wird davon ausgegangen, dass Sie einen Gmail-Account als bevorzugtes E-Mail-Konto verwenden. Auf dem Startbildschirm befindet sich bereits das charakteristische Programmsymbol (Abbildung 24.38). Über ein weiteres E-Mail-Symbol können Sie auch Exchange-, POP3- oder IMAP-Konten einrichten. Die Konfiguration erfolgt auf die gleiche Weise wie bei E-Mail-Programmen für den Desktop-PC. Das umfasst auch die Angabe einer Portnummer und einer Verschlüsselungsmethode wie SSL oder TLS (Abbildung 24.39), sofern der Server diese nicht automatisch konfiguriert.

Hinweis

Die neuesten Android-Versionen rufen die Portnummern und Protokolle einfach vom E-Mail-Server ab, um sie zu konfigurieren, so wie es E-Mail-Programme für den Desktop auch tun. Der Vorgang ist zwar automatisiert, aber die Portnummern gehören zu den Lernzielen der CompTIA, deshalb müssen Sie diese kennen.

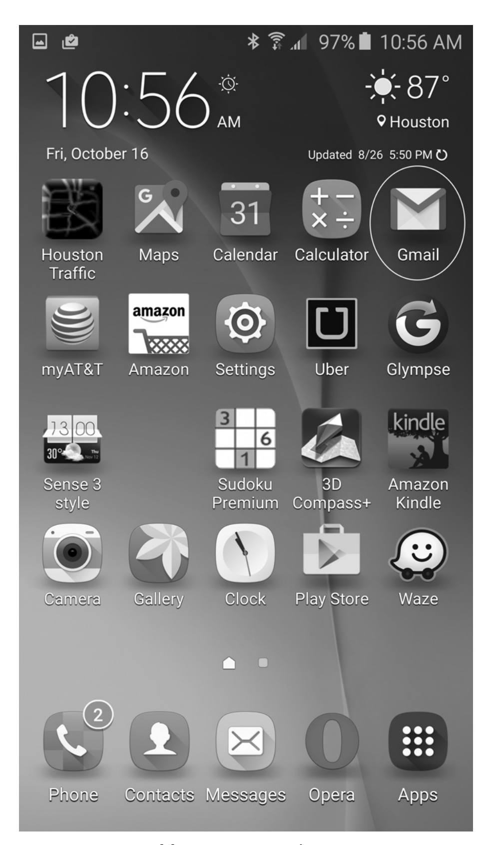


Abb. 24.38: Gmail-App

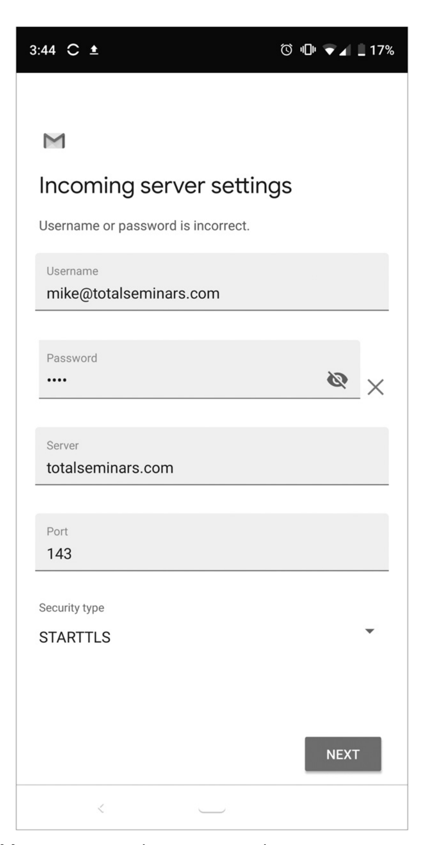


Abb. 24.39: Einrichten eines sicheren IMAP-Kontos

In der CompTIA A+-Prüfung geht es beim Thema E-Mail-Einstellungen ziemlich zur Sache, insbesondere was die TCP-Portnummern der verschiedenen E-Mail-Protokolle betrifft. Sie wurden in den vorhergehenden Kapiteln bereits erwähnt, sind hier jedoch noch einmal kurz zusammengefasst:

- POP3 verwendet TCP-Port 110
- IMAP4 verwendet TCP-Port 143
- SMTP verwendet TCP-Port 25

Viele Server blockieren diese Ports, und wenn Sie die sicheren Varianten der Protokolle verwenden möchten, müssen Sie andere Portnummern benutzen. Ich habe keine Ahnung, ob die CompTIA nach den Portnummern der sicheren Varianten von POP3, IMAP4 und SMTP fragt, aber hier sind sie:

- Sicheres POP3 verwendet TCP-Port 995
- Sicheres IMAP4 verwendet TCP-Port 993
- Sicheres SMTP verwendet TCP-Port 465 oder 587

Je nachdem, wie der Mailserver eingerichtet ist, sind möglicherweise noch weitere Angaben erforderlich, wie beispielsweise *S/MIME* (*Secure/Multipurpose Internet Mail Extension*), die dazu verwendet werden, die Einstellungen für digitale E-Mail-Signaturen und Kontakte des firmenweiten Adressbuchs zu konfigurieren.

Wichtig

Die vorkonfigurierten E-Mail-Dienste von Google, Yahoo!, Outlook.com und iCloud sollten Sie kennen. Merken Sie sich auch die Einstellungen für POP3, IMAP4, Portnummern und SSL-Einstellungen, sowie die Konfiguration von Exchange und S/MIME.

24.3.6 Synchronisierung

Bei mobilen Geräten gab es schon immer ein bestimmtes Problem: die darauf befindlichen Daten. Die Kontakte auf dem mobilen Gerät sollen doch bitteschön mit denen auf dem Desktop-PC oder den online gespeicherten identisch sein. Die Leute haben auch keine Lust, E-Mails auf dem mobilen Gerät zu bearbeiten und dann online die gleichen Änderungen erneut vornehmen zu müssen. Und der Kalender soll natürlich auch überall den gleichen Inhalt besitzen. Kurzum: Wenn Sie ein mobiles Gerät besitzen, brauchen Sie auch eine Methode, um all diese Daten miteinander zu synchronisieren, damit Kontakte, E-Mails, Kalender usw. auf allen Geräten miteinander übereinstimmen.

Smartphones und Tablets lassen sich mit dem Desktop-PC lokal oder mit Cloud-Diensten über das Internet *synchronisieren*, um Daten und Dateien auf dem neuesten Stand zu halten. Dazu gehören persönliche Dokumente, Lesezeichen, Kalendereinträge, Daten sozialer Netzwerke, E-Books und sogar Angaben zum Aufenthaltsort. Für ältere Geräte (wie etwa BlackBerry oder Palm Pilot) gab es spezielle Synchronisierungssoftware, die auf dem PC installiert wurde und zum Abgleich von Kontakten, Kalender usw. diente. Heutzutage verwenden die Geräte vergleichbare Software oder synchronisieren sich über Cloud-Dienste.

Die verschiedenen Tablets und Smartphones verwenden zur Synchronisierung unterschiedliche Methoden – je nach Hersteller und erforderlicher Software. iOS-Geräte verwenden Apples iCloud zum Synchronisieren von iPhone, iPad und Macs. Android-Geräte,können die vielfältigen Dienste von Google nutzen, um bestimmte Einstellungen, Apps, Softwareaktualisierungen usw. zu synchronisieren. In manchen Fällen wird auch gar keine spezielle App zur vollständigen Synchronisierung benötigt. Stattdessen könnten auch mehrere einzelne Apps jeweils nur bestimmte Teile des Datenbestands synchronisieren. Ein Podcast-Programm könnte beispielsweise bei der Synchronisierung Daten wie abonnierte Shows berücksichtigen. Ältere iOS-Geräte mussten zur Synchronisierung mit einem Laptop oder Desktop Apples iTunes verwenden. Das funktioniert zwar immer noch, aber die meisten Benutzer lassen diese Aufgabe im Hintergrund durch iCloud erledigen.

Wichtig

Die Synchronisierung ermöglicht es mobilen Geräten, alle wichtigen Informationen auf dem neuesten Stand zu halten. Sie sollten wissen, welche Art von Daten typischerweise synchronisiert wird: Kontakte, Programme (Apps), E-Mail, Bilder, Musik, Videos, Kalenderdaten, Lesezeichen, Dokumente, Aufenthaltsorte, Daten sozialer Netzwerke, E-Books und Kennwörter. Das ist wirklich eine ganze Menge!

Synchronisierung mit dem Auto

Die Autohersteller wissen ganz genau, dass Sie beim Autofahren telefonieren. Das ist zwar gefährlich, denn eine interessante Unterhaltung kann Sie von der Umgebung und anderen zwei Tonnen schweren Todesmaschinen ablenken, aber dennoch machen es alle. Moderne Autos sind mit Sprachkommunikationssystemen ausgestattet, die per Bluetooth mit dem Smartphone verbunden werden (Abbildung 24.40). Damit ist es unter anderem möglich, über Sprachbefehle Anrufe zu tätigen. Zudem ist das Smartphone meist mit dem Navigationssystem des Fahrzeugs verknüpft, damit es Ihnen helfen kann, von A nach B zu gelangen.



Abb. 24.40: Anruf per iPhone mit dem Unterhaltungssystem eines Autos

Sie sind auch nicht mehr nur auf den Desktop-PC beschränkt. Dank immer schnellerer Mobilfunk- und WLAN-Technologien können Sie auch größere Datenmengen über die Cloud synchronisieren. Alle Smartphone-Hersteller setzen eigene Versionen der Cloud-Technologien ein. Sie können sich ein Benutzerkonto einrichten und die Cloud verwenden, um die persönlichen Daten auf Ihrem Gerät dort zu speichern. Apple hat iCloud, Microsoft hat One Drive, Google hat Google Drive und auch viele Hersteller von Android-Geräten bieten solche Dienste an.

Außerdem gibt es unabhängige Cloud-Anbieter, die es neben dem Speichern persönlicher Daten ermöglichen, diese mit anderen zu teilen. Dropbox ist wohl das beste Beispiel für solche Anbieter, aber es gibt noch viele andere. Die meisten dieser Dienste treffen gewisse Sicherheitsmaßnahmen zum Schutz der Daten und verlangen die Eingabe von Benutzername und Kennwort zur Authentifizierung. Einige Anbieter gestatten es auch, die Daten verschlüsselt in der Cloud zu speichern.

Das Synchronisieren mit einem Desktop-PC (oder einem Laptop) hat sowohl Vor- als auch Nachteile. Von Vorteil ist, dass die Daten vollständig unter Ihrer Kontrolle stehen und Sie bei Bedarf eine Verschlüsselung Ihrer Wahl verwenden können. Sie können die Daten sogar auf externen Datenträgern speichern und diese an einem anderen Ort lagern, um im Notfall auf eine Sicherheitskopie zurückgreifen zu können. Nachteilig ist, dass Sie in der Lage sein müssen, sich mit dem Computer zu verbinden – was problematisch sein kann, wenn Sie ihn nicht mitnehmen können.

Die Synchronisierung über die Cloud besitzt ebenfalls Vor- und Nachteile. Wenn eine ordentliche Mobilfunk- oder WLAN-Verbindung verfügbar ist, können Sie überall eine Synchronisierung durchführen. Sie sollten allerdings vorsichtig sein, wenn Sie unsichere öffentliche WLANs nutzen, denn hier besteht die Möglichkeit, dass Ihre Daten mitgehört werden. Außerdem stehen die Daten nicht mehr unter Ihrer alleinigen Kontrolle, wenn Sie die Cloud nutzen. Sie sind auf Gedeih und Verderb den Sicherheitsmechanismen und Datenschutzrichtlinien Ihres Anbieters ausgeliefert. Sie müssen die vorhandenen Schutzmaßnahmen akzeptieren, wie etwa die Stärke (oder Schwäche) der eingesetzten Verschlüsselung. Außerdem müssen Sie sich den Datenschutzrichtlinien beugen, die es möglicherweise gestatten, Ihre personenbezogenen Daten an Strafverfolgungsbehörden oder zu Werbezwecken an

Dritte weiterzugeben. Manche Anbieter beschränken auch Art und Umfang der gespeicherten Daten, so könnten z.B. bestimmte Arten von Mediendateien (Musik, Videos, Software) nicht gestattet sein, um Urheberrechtsverletzungen zu verhindern.

Alle diese Überlegungen müssen Sie in Betracht ziehen, wenn Sie entscheiden, ob Sie Ihr mobiles Gerät mit einem PC oder mit der Cloud synchronisieren möchten – oder mit beiden.

Wichtig

In den Lernzielen der Prüfung ist im Zusammenhang mit der Synchronisierung eine merkwürdige Formulierung aufgetaucht: »gegenseitige Authentifizierung für mehrere Dienste«. Die Bedeutung ist unklar und es ist schwer zu sagen, was die CompTIA hier hören möchte. Eine entsprechend programmierte App ermöglicht es, sich per Smartphone oder Tablet mit einem anderen Benutzerkonto anzumelden, an dem Sie bereits angemeldet sind, wie etwa Google, Apple-ID, Facebook, Twitter etc. Das Verfahren, sich mithilfe einer aktiven authentifizierten Sitzung bei einem dieser Dienste bei einem anderen Dienst anzumelden, wird als *Single-Sign-On* (SSO) bezeichnet.

Probleme beim Synchronisieren

Das bei der Synchronisierung am häufigsten auftretende Problem ist, dass sie unvollständig bleibt. Die Ursache dafür können Schwierigkeiten bei der Herstellung der Verbindung, das Gerät selbst oder auch Probleme der entfernten Infrastruktur sein. Bei der Synchronisierung kann es dann dazu kommen, dass E-Mails nur teilweise oder sogar doppelt heruntergeladen werden. Wenn keine stabile Verbindung zustande kommt, versucht das Gerät immer wieder, die Synchronisierung durchzuführen und lädt dann dieselben E-Mails mehrfach herunter. Auch das Herunterladen von Patches oder Aktualisierungen kann scheitern. Meistens liegt das an der WLAN- oder Mobilfunkverbindung und das Problem lässt sich beheben, indem man einen Bereich aufsucht, in dem der Empfang besser ist. Sollte es Schwierigkeiten beim Hochladen von Daten gibt, ist das leider nicht immer hilfreich.

In manchen Fällen können auch andere Dinge eine erfolgreiche Synchronisierung verhindern, etwa eine misslungene Authentifizierung, inkompatible Betriebssystemversionen oder fehlerhafte Einstellungen. Wenn die Synchronisierung trotz stabiler Verbindung nicht klappen will, sollten Sie überprüfen, ob das Problem vielleicht am anderen Ende der Verbindung zu suchen ist, etwa beim Mailserver oder dem Zugangspunkt zum betroffenen Unternehmensnetzwerk. Eine gescheiterte Authentifizierung oder fehlerhafte Einstellungen für den Zugriff auf den Zugangspunkt können die Synchronisierung ebenfalls verhindern.

Wenn es Problem bei der Synchronisierung gibt, sollten Sie einer weiteren Problematik Beachtung schenken. Unter Umständen findet eine Synchronisierung mit verschiedenen Quellen statt, z.B. mit einem Firmenserver, einem App Store des Herstellers, mit E-Mail-Diensten wie Gmail und Yahoo!, oder sonstigen Drittanbietern von Diensten bzw. Cloud-Speicherplatz. Sie müssen in diesem Fall in Betracht ziehen, dass für die verschiedenen Anbieter unterschiedliche Konfigurationseinstellungen (z.B. für die Verschlüsselung) erforderlich sein können und es dadurch zu Konflikten kommt. In Unternehmensumgebungen obliegt es dem für die Verwaltung mobiler Geräte zuständigen Team, hier eine geeignete Strategie auszuarbeiten, die dafür sorgt, dass es möglichst keine Konflikte zwischen den verschiedenen Synchronisierungsquellen gibt.

iTunes und iCloud

iPhone und iPad können auf Mac und PC mittels *iTunes* synchronisiert werden. Alle Daten (Musik, Videos, Kontakte, Bilder, E-Mails, Apps usw.) können lokal gespeichert werden. Darüber hinaus können Sie mit iTunes eine Sicherungskopie der auf Ihrem iPhone oder iPad befindlichen Apps erstellen. Falls Ihrem Gerät etwas zustößt, ist die Wiederherstellung besonders einfach, da nur eine Datenquelle zu berücksichtigen ist. Wenn Sie beispielsweise ein Apple-Gerät ersetzen müssen, brauchen Sie das neue Gerät einfach nur mit iTunes zu synchronisieren. Dabei werden sämtliche Dateien, Kontaktdaten und Apps auf das neue Gerät kopiert.

Wichtig

iTunes funktioniert auf so ziemlich jedem Rechner, auf dem auch macOS oder Windows läuft. Als Systemanforderungen der neuesten iTunes-Version (64 Bit) nennt Apple mindestens Windows 7 (64 Bit) oder neuer und einen Intel- oder AMD-Prozessor mit 1 GHz und Unterstützung für SSE2 sowie 512 MB RAM. Mit einem 1-GHz-Prozessor und einer 16-Bit-Soundkarte können Sie zwar Musik abspielen, zur Wiedergabe eines hochauflösenden Videos ist jedoch ein 2,4-GHz-Prozessor mit zwei (oder mehr) Kernen erforderlich. Für einen Mac ist macOS 10.10.5 oder neuer notwendig. Weitere Informationen finden Sie unter `http://www.apple.com`.

Mit iCloud können Sie all Ihre iPhone- oder iPad-Daten sichern und von überall darauf zugreifen Dazu gehören neben den Einkäufen im iTunes Store auch Kontakte, Kalender, Erinnerungen usw.

Android und Gmail

Eine zentrale Anwendung zur Synchronisation wie iTunes für Apple-Geräte gibt es bei mobilen Geräten mit Android nicht. Stattdessen synchronisieren sie sich über das Internet. Welche Daten synchronisiert werden können, hängt von den von Ihnen genutzten Google-Diensten und den installierten Apps ab. Zu den üblichen Optionen gehören App-Daten, Kontakte, Kalender, E-Mail, bei Google Play erworbene Medien, bei Google Drive oder Google Pictures gespeicherte Dateien und mehr. Was alle anderen Daten betrifft, können Sie ein Android-Gerät wie einen ziemlich dicken USB-Speicherstick verwenden: Dateien werden per Drag&Drop in die entsprechenden Ordner auf dem Tablet oder Smartphone kopiert.

24.3.7 Verbindungen und Anschlüsse

Mobile Geräte wären nicht besonders nützlich, wenn sie nicht mit der Außenwelt auf möglichst vielfältige Weise Kontakt aufnehmen könnten. In diesem Abschnitt werden die verschiedenen Technologien und Verbindungsmöglichkeiten beleuchtet, die beim Datenaustausch mit mobilen Geräten zum Einsatz kommen.

Micro-USB/Mini-USB

Falls Ihr Android-Gerät vor 2017 hergestellt wurde, besitzt es sehr wahrscheinlich einen Micro- oder Mini-USB-Anschluss, um es aufzuladen, mit dem PC zu verbinden und zu synchronisieren. Micro- und Mini-USB-Anschlüsse waren bei den meisten Android-Geräten Standard. Das soll aber nicht heißen, dass diese nicht auch proprietäre Anschlüsse verwenden. Das Betriebssystem stammt zwar von Google, einige Hersteller verwenden jedoch eigene Anschlüsse oder Stecker, die nur bei diesem Hersteller erhältlich sind.

Lightning-Anschluss

Zusammen mit dem iPhone 5 stellte Apple den aktuellen proprietären *Lightning*-Anschluss vor. Er ersetzt den älteren 30-poligen Anschluss, den Apple bei vorhergehenden iPhones und iPads verwendete. Der Lightning-Stecker besitzt auf jeder Seite acht Kontakte (Abbildung 24.41). Beim Anschließen spielt die Ausrichtung des Steckers keine Rolle – es gibt keine Ober- oder Unterseite wie beim herkömmlichen USB-Stecker. Aufgrund der proprietären Natur des Anschlusses sind Lightning-Kabel teurer als USB-Kabel. Der Anschluss wird an andere Hersteller lizenziert und enthält einen Chip, der ihn als echten Lightning-Stecker identifiziert, um die massenhafte Produktion gefälschter Lightning-Kabel zu verhindern. Kabel ohne diesen Chip funktionieren oft nicht oder sind nur von begrenztem Nutzen.



Abb. 24.41: Der Lightning-Anschluss

Wichtig

Der Lightning-Anschluss ist ein Paradebeispiel für einen proprietären, herstellerspezifischen Anschluss. Er wird nur von iOS-Geräten zur Stromversorgung und Datenübertragung verwendet. Android-Geräte nutzen standardisierte, herstellerunabhängige Anschlüsse.

USB Typ C

USB Typ C ist die jüngste Inkarnation von USB-Steckern (Abbildung 24.42). Er ist bei Android-Geräten schnell zu einem De-facto-Standard geworden, was sehr erfreulich ist, denn man braucht für Laptop und Smartphone nur noch ein Ladegerät. Tatsächlich setzt sogar Apple den Typ-C-Stecker bei den neuesten iPad Pros ein, weil er zu einer Vielzahl von Peripheriegeräten kompatibel ist und dank seiner Fähigkeit, höhere Ströme zu verkraften, schnelleres Laden ermöglicht.

Wie beim Lightning-Stecker spielt die Ausrichtung des Steckers beim Anschließen keine Rolle. Der Anschluss kann USB 3.1 mit Datenübertragungsraten von bis zu sehr schnellen 10 Gbps unterstützen (muss es aber nicht). Die Verwendung des Typ-C-Steckers bedeutet jedoch nicht, dass eine bestimmte USB-Version zum Einsatz kommt. Manche Geräte nutzen den Stecker für USB-2.0-Verbindungen.



Abb. 24.42: USB-Typ-C-Stecker

Wichtig

Die Prüfung hat wahrscheinlich Micro- und Mini-USB-, USB-Typ-C- und Lightning-Anschlüsse zum Thema. Sie sollten deren Merkmale und Unterschiede kennen.

Bluetooth

Bluetooth sowie die Konfiguration und Kopplung wurden in Kapitel 20 bereits ziemlich ausführlich beschrieben. An dieser Stelle betrachten wir kurz, wie das Ganze bei Smartphones und Laptops funktioniert. Aktivieren Sie auf dem Smartphone bzw. dem Tablet zunächst Bluetooth, wenn es noch nicht aktiviert ist. Wie das erfolgt, unterscheidet sich von Gerät zu Gerät, die Funktion sollte aber in den Einstellungen zu finden sein. Schalten Sie jetzt das Bluetooth-Gerät ein (oder vergewissern Sie sich, dass Bluetooth aktiviert ist, falls das Gerät schon eingeschaltet ist). Auf Ihrem mobilen Gerät wählen Sie dann das entsprechende Gerät zum Koppeln aus und geben gegebenenfalls die PIN (*Personal Iden-*

tification Number) ein. Bei einer Bluetooth-Tastatur zeigt das Smartphone oder das Tablet beispielsweise eine Reihe von Zeichen oder Ziffern an, die Sie dann eintippen müssen. Sobald Sie das erledigt haben, werden die Geräte miteinander verbunden (Abbildung 24.43).

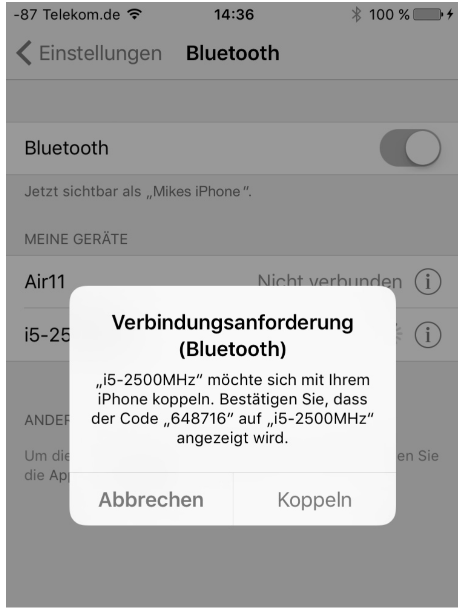


Abb. 24.43: Kopplung zweier Bluetooth-Geräte

Wichtig

Beim Koppeln zweier Bluetooth-Geräte ist nicht immer eine PIN erforderlich, es müssen jedoch stets auf *beiden* Geräten bestimmte Aktionen durchgeführt werden, damit die Kopplung zustande kommt.

Nach der Kopplung sollten Sie die Verbindung mit dem neuen Bluetooth-Gerät überprüfen. Im Falle einer Tastatur könnten Sie etwa eine Notizen-App öffnen und etwas eingeben, um zu prüfen, ob die Tastatur funktioniert.

Hinweis

Für gewöhnlich ist Bluetooth standardmäßig deaktiviert, um den Akku nicht unnötig zu belasten. Das Suchen nach Bluetooth-Geräten und die Kopplung selbst benötigen Energie. Aktivieren Sie Bluetooth also nur, wenn Sie es auch verwenden, und rechnen Sie mit einer geringeren Akkulaufzeit.

NFC

Bei der *Nahfeldkommunikation* (*NFC – Near Field Communication*) werden in die Geräte eingebaute Chips verwendet, die elektromagnetische Felder erzeugen, wenn zwei Geräte sich in unmittelbarer Nähe befinden. Die typische Reichweite einer NFC-Datenübertragung beträgt nur wenige Zentimeter. Die kommunizierenden Geräte müssen sich also sehr nahe sein oder einander sogar berühren und können zum Übertragen von Informationen wie Kontakten, kleinen Dateien oder den für Bezahlvorgänge erforderlichen Daten (wie bei Apple Pay oder Google Pay) genutzt werden. Diese Technologie findet bei neuen Geräten zunehmend Verbreitung. Gleiches gilt für die zu ihrer Unterstützung erforderlichen Anwendungen und Infrastrukturen.

Magnetkarten- und Chipkartenleser

Händler können einen Magnetkarten- oder Chipkartenleser an einem Smartphone anschließen, um schnelle Kreditkartentransaktionen über das Mobilfunknetz zu ermöglichen (Abbildung 24.44). Diese Technologie hat es großen wie kleinen Händlern ermöglicht, auf Registrierkassen zu verzichten. Ein Handel kann jetzt überall dort stattfinden, wo Güter oder Dienstleistungen gegen Geld eingetauscht werden sollen. Beim diesjährigen Texas Renaissance Festival verfügten sämtliche Händler über am Smartphone angeschlossene Kreditkartenleser, um das Geld des Totalsem-Teams anzunehmen, das sich dort verkleidete und mitspielte (Abbildung 24.45). Hurra!



Abb. 24.44: Am Smartphone angeschlossener Magnetkartenleser



Abb. 24.45: Das Totalsem-Team beim Texas Renaissance Festival

Infrarot

Infrarot wurde weitgehend von schnelleren Technologien abgelöst, wie Bluetooth und dem 802.11-Standard. Früher wurden Infrarot-Signale (IR) zur Datenübertragung zwischen mobilen Geräten verwendet, beispielsweise zwischen Laptops und älteren PDAs. Bei den ersten PANs (*Personal Area Networks*) kam Infrarot zum Einsatz. Die Technologie nutzt den IrDa-Standard (*Infrared Data Association*) und wurde seinerzeit für Verbindungen mit Fernbedienungen, Druckern, Mäusen, Digitizern und anderen seriellen Geräten verwendet. IrDa erfordert eine Sichtverbindung, sodass sich die Geräte einander direkt gegenüber und in unmittelbarer Nähe (manchmal nur wenige Zentimeter) befinden müssen. Die Datenübertragungsrate ist sehr niedrig.

Hinweis

Wenn ein modernes Smartphone oder Tablet eine Infrarot-Abdeckung besitzt, verbirgt sich dahinter fast mit Sicherheit ein sogenannter *Infrarot-Blaster*, der kräftige Infrarot-Signale senden (aber nicht empfangen) kann. Es wird zwar nach wie vor eine Sichtverbindung zum anderen Gerät benötigt, aber die Reichweite ist größer.

Hotspots und Tethering

Ein mobiler Hotspot ist ein kleines Gerät, das über eine Technologie wie 3G, 4G oder LTE auf das Mobilfunknetz zugreifen kann und diese Verbindung WLAN-fähigen Geräten bereitstellt. Die meisten dieser Geräte sind bei Anbietern wie T-Mobile, AT&T, Sprint oder Verizon erhältlich und für den Zugriff auf das jeweilige Netz ausgelegt. Im Wesentlichen handelt es sich um einen drahtlosen Router, der den Datenverkehr zwischen Mobilfunknetz und WLAN vermittelt und etwa fünf bis zehn anderen Geräten gleichzeitig eine Internetverbindung zur Verfügung stellt.

Je nach Anbieter können aber auch viele Smartphones und Tablets als Hotspots fungieren, wie Sie aus Kapitel 21 wissen. Diese Art der Nutzung wird als *Tethering* bezeichnet. Manche Mobilfunkverträge umfassen die Verwendung als Hotspot, einige Anbieter bewerten die so genutzte Bandbreite jedoch eigenständig und beschränken die über Tethering nutzbare Datenmenge.

Um ein Gerät als Hotspot zu verwenden, müssen Sie für gewöhnlich in den Einstellungen einen Router aktivieren, der die Daten des Mobilfunknetzes an das WLAN weiterleitet. Andere WLAN-fähige Geräte sehen das Gerät dann als drahtlosen Router. Sie können ein Kennwort vergeben, damit sich nicht jedermann mit Ihrem Hotspot verbinden darf. Abbildung 24.46 zeigt ein iPhone, das als portabler Hotspot arbeitet.

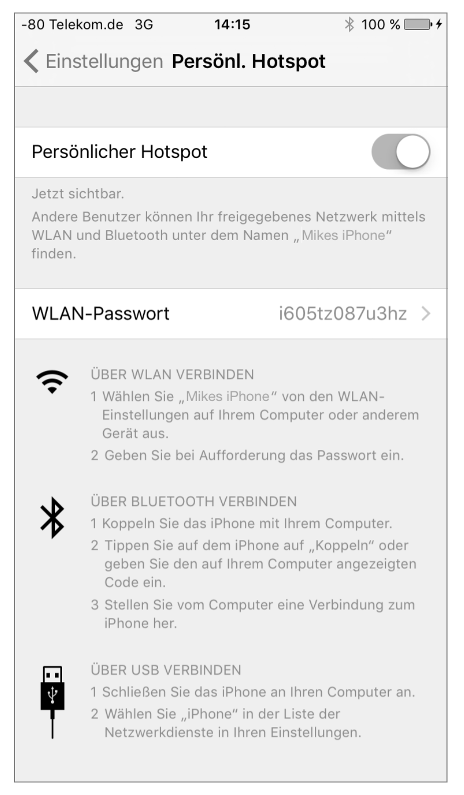


Abb. 24.46: iPhone als persönlicher Hotspot

Zubehör

Zubehör für mobile Geräte gibt es in allen erdenklichen Varianten und mit einer großen Bandbreite an Funktionen. Zum beliebtesten Zubehör gehören Geräte, die sich drahtlos verbinden lassen, typischerweise über Bluetooth. Bluetooth-Headsets oder hochwertige externe Lautsprecher zum Musikhören und Chatten mit Freunden sind an der Tagesordnung.

Per USB oder Bluetooth verbundene Gamepads sind ebenfalls gebräuchlich und machen die mobilen Geräte so zu einer echten Spieleplattform. Es gibt sogar Tablets mit eingebauten Steuerelementen, die speziell zum Spielen gedacht sind. Das NVIDIA SHIELD ist ein spezialisiertes Android-Gerät, das als Spieleplattform dient und ansonsten das Gleiche leistet wie andere Android-Tablets.

Manche Android- und Microsoft-Geräte bieten die Möglichkeit, externe Speicherkarten (Mini- oder Micro-USB-Karten) zu verwenden und so die Speicherkapazität zu erhöhen. Apple-Geräte bieten diese Möglichkeit bislang nicht.

Neben den gerade genannten Gerätschaften gibt es Zubehör, auf das kein Benutzer verzichten sollte, wie etwa Ersatzakkus (sofern Ihr Gerät ein Batteriefach besitzt, was bei mobilen Geräten oft nicht der Fall ist), eine *Powerbank* zum Aufladen des internen Akkus, oder ein Ladegerät bzw. Ladekabel. Mit dem Ladegerät können Sie das Gerät an einer Steckdose aufladen; das Ladekabel wird zum Aufladen an einem Computer oder Laptop angeschlossen.

Es gibt auch Ladegeräte, die drahtlos arbeiten. Sie legen Ihr Gerät einfach auf eine spezielle Ablage und das Gerät wird per Induktion aufgeladen. Wie das genau funktioniert, hängt auch davon ab, ob das Gerät für drahtloses Laden ausgelegt ist oder ob diese Fähigkeit durch Zubehör bereitgestellt wird. Jedenfalls wird ein elektromagnetisches Feld erzeugt, über das Energie an eine Antenne im Gerät übertragen wird. Auch wenn es sich um eine drahtlose Technologie handelt, bemisst sich die Reichweite nur in Zentimetern, und das Laden funktioniert am besten, wenn sich das Gerät auf der Ablage befindet.

Auf diesem Markt hat sich der Qi-Standard des WPC (*Wireless Power Consortium*) etablieren können. Apple hat sich 2017 dazu entschlossen, den Qi-Standard zu unterstützen, und trat dem WPC bei. Das hat das Schicksal konkurrierender Standards endgültig besiegelt.

Wichtig

Wenn ein Gerät herausnehmbare wiederaufladbare Batterien verwendet, lassen sie sich mit einem Batterieladegerät wiederaufladen. Wenn Sie Ersatzbatterien parat haben, können Sie Ihr Gerät sofort weiter benutzen. Legen Sie die wiederaufladbaren Batterien in das Ladegerät ein und schließen Sie es an einer Steckdose an.

Je nach verwendetem Gerät kann weiteres Zubehör sinnvoll sein, z.B. Dockingstationen des Geräteherstellers (typischerweise für Tablets, wie die in Kapitel 23 vorgestellten) oder sogar Kreditkartenlesegeräte, die es kleineren Geschäften ermöglichen, Zahlungen per Kreditkarte mit dem mobilen Gerät entgegenzunehmen. Ich habe beispielsweise schon öfter in Geschäften gesehen, dass in der Kopfhörerbuchse eines iPads ein Kreditkartenleser steckte.

Ein weiteres unverzichtbares Zubehör ist eine Schutzhülle oder Abdeckung für das Gerät. Es gibt Designerstücke mit allen erdenklichen darauf abgebildeten Motiven oder stabile Gehäuse, die dafür ausgelegt sind, dass die darin befindlichen Geräte Stürze heil überstehen. Schutzabdeckungen für den Bildschirm sind ebenfalls in vielfältiger Form erhältlich. Das Spektrum reicht von wenig solidem Plastik bis hin zu gehärtetem Spezialglas, das die Geräte vor Kratzern und Stößen schützt. Es gibt Gehäuse und Hüllen aus Kunststoff, Gummi, Leder, Holz und Metall. Manche davon sind sogar wasserdicht und ermöglichen es abenteuerlustigen Benutzern, ihre Smartphones mitzunehmen, wenn sie im Meer tauchen oder Wildwasserfahrten unternehmen.

Ich habe nur einige wenige Zubehörteile für mobile Geräte erwähnt, es gibt allerdings buchstäblich Hunderte weitere. Zu vielen Erweiterungen gehört eine App, die es erst ermöglicht, das betreffende Zubehör überhaupt zu benutzen oder es richtig auszureizen.

24.4 Wiederholung

24.4.1 Fragen

1. Wodurch werden analoge Videos und Sounds von mobilen Geräten in digitale Videos und Sounds umgewandelt?

   A. Kalibrierung

   B. SDK

   C. Virtueller Assistent

   D. Digitizer

2. Johannes hat auf seinem iPad ein hochauflösendes Bild von seinem zweijährigen Sohn und dem Hund der Familie gespeichert. Das Bild wird jedoch auf dem Bildschirm sehr klein dargestellt, deshalb möchte er hineinzoomen, damit er den Gesichtsausdruck seines Sohnes erkennen kann. Wie kann er das erreichen?
   A. Bild mit der Maus anklicken, um es auszuwählen, und dann mit dem Scrollrad der Maus hineinzoomen.
   B. Mit dem Zeigerfinger das Gesicht seines Sohns antippen.
   C. Bild antippen und lange gedrückt halten und im Einblendmenü ZOOM auswählen.
   D. Bild mit Daumen und Zeigefinger antippen und auseinanderspreizen, um hineinzuzoomen.
3. Welche Bildschirmtechnologie verwendet keine Hintergrundbeleuchtung?
   A. BYOD
   B. LCD
   C. LED
   D. OLED
4. Womit können Behörden Ihren Aufenthaltsort zu einem bestimmten Zeitpunkt bestimmen, wenn Sie ein Smartphone oder Tablet verwenden?
   A. Mehrfaktor-Authentifizierung
   B. Geotracking
   C. Google Earth
   D. Authentifizierungsanwendungen
5. Wie wird die Kopplung zwischen Bluetooth-Tastatur und Tablet durchgeführt?
   A. Beim Tablet Bluetooth aktivieren, Bluetooth-Gerät einschalten, auf dem Tablet auswählen und den PIN-Code eingeben
   B. Bluetooth-Gerät einschalten, auf dem Tablet auswählen und PIN-Code eingeben
   C. Auf dem Tablet nach Bluetooth-Geräten suchen und unter den Geräteoptionen KOPPELN antippen
   D. Beim Tablet Bluetooth aktivieren, Bluetooth-Gerät einschalten, auf dem Tablet auswählen und unter den Geräteoptionen KOPPELN antippen.
6. Welche der genannten Abkürzungen beschreibt eine 15-stellige Nummer zur eindeutigen Identifizierung eines mit einem Mobilfunknetz verbundenen Geräts?
   A. IMEI
   B. GSM
   C. ICCID
   D. IMSI
7. Maria war auf einer Kreuzfahrt zu den Bahamas und hat jetzt von ihrem Mobilfunkanbieter eine Rechnung über 1000 Euro erhalten. Was könnte passiert sein?
   A. Maria hat auf dem Kreuzfahrtschiff das WLAN der Reederei für die Internetverbindung genutzt.
   B. Maria hat auf den Bahamas für ihre Internetverbindung einen anderen.Mobilfunkanbieter verwendet.
   C. Maria hat ihr Smartphone für Glücksspiele im Internet genutzt, und das missfällt ihrem Mobilfunkanbieter.
   D. Der Rechnungsbetrag wird nach Auslandsreisen in der jeweiligen Landeswährung angegeben. Wenn man den Betrag in Euro umrechnet, ist er nicht höher als sonst.

8. Klaus hat sich gerade einen ziemlich teuren Bildband gekauft und mittels der auf seinem Smartphone gespeicherten Kreditkartendaten bezahlt. Welche Technologie hat er beim Bezahlen verwendet?
   A. Bildschirmsperre durch eine Geste
   B. WLAN-Telefonie
   C. NFC
   D. BitLocker To Go
9. Welche Informationen benötigen Sie, um auf einem Android-Tablet ein IMAP-Konto einzurichten?
   A. POP3-Servername und DNS-Bezeichnung
   B. Benutzername und Kennwort
   C. Benutzername, Kennwort und die Adressen der Server für ein- und ausgehende E-Mails
   D. Exchange-Servername, Benutzername und Kennwort.
10. Welches Betriebssystem ermöglicht es Herstellern, das Aussehen und die Bedienung ohne Einschränkungen zu gestalten?
   A. Android
   B. Blackberry
   C. iOS
   D. Windows Phone

24.4.2 Antworten

1. **D.** Digitizer konvertieren Videos und Sounds von analog zu digital oder wandeln die Bewegungen der Finger auf dem Bildschirm in digitale Signale um.
2. **D.** Johannes sollte das Bild mit Daumen und Zeigefinger antippen und auseinanderspreizen, um hineinzuzoomen.
3. **D.** OLED verwendet keine Hintergrundbeleuchtung.
4. **B.** Durch Geotracking können Sie bzw. Ihr GPS-fähiges Gerät lokalisiert werden.
5. **A.** Um eine Bluetooth-Tastatur mit einem Tablet zu koppeln, müssen Sie beim Tablet Bluetooth aktivieren, das Bluetooth-Gerät einschalten, es in den EINSTELLUNGEN des Tablets auswählen und den PIN-Code eingeben.
6. **A.** Die IMEI (*International Mobile Equipment Identity*) ist eine 15-stellige Nummer, die mit einem Mobilfunknetz verbundene Geräte, typischerweise Smartphones oder Tablets, eindeutig identifiziert.
7. **B.** Marias Smartphone hat sich auf den Bahamas über einen anderen Mobilfunkanbieter mit dem Internet verbunden.
8. **C.** Klaus hat seinen Bildband vermutlich per NFC bezahlt. Diese Technologie ermöglicht es, Zahlungen mittels der auf einem Smartphone gespeicherten Kreditkartendaten vorzunehmen.
9. **C.** Um auf einem Android-Tablet ein IMAP-Konto einzurichten, sind Benutzername, Kennwort und die Adressen der Server für ein- und ausgehende E-Mails erforderlich.
10. **A.** Google Android ist quelloffen und ermöglicht es den Herstellern, eigene Versionen für ihre Geräte zu entwickeln.

Wartung und Pflege von mobilen Geräten | 25

Themen in diesem Kapitel:

- Fehlerbehebung bei mobilen Geräten
- Grundlegende Sicherheitsaspekte
- Sicherheitsprobleme bei mobilen Geräten

Mobile Geräte sind vollgepackt mit hochgradig integrierter Hardware und nicht dafür ausgelegt, dass Benutzer sie aufrüsten. Die Betriebssysteme orientieren sich am Bedarf bei mobilen Geräten. Aufgrund dieser Unterschiede zu normalen PCs liegt es in der Natur der Sache, dass sich die Fehlerbehebung und die Sicherheitsrichtlinien von mobilen Geräten und Desktop-Computern stark unterscheiden. Andere mobile Geräte sind davon ebenfalls in gewissem Maße betroffen.

In diesem Kapitel sehen wir uns zunächst die allgemeine Fehlerbehebung an und erörtern dann die Sicherheitsmaßnahmen für die im mobilen Marktsegment gängigen Geräte. Am Ende dieses Kapitels betrachten wir verschiedene Aspekte der Fehlerbehebung: Bedrohungen erkennen, Sicherheitsmaßnahmen treffen und Probleme mit bestimmten Anwendungen beheben. Die CompTIA stellt gern Fragen zu diesem Themenkreis, rechnen Sie also mit praxisnahen Szenarien, wenn es um Sicherheitsprobleme und Fehlerbehebung bei Anwendungen geht.

1001/1002

25.1 Fehlerbehebung bei mobilen Geräten

In den Lernzielen der CompTIA A+-Zertifizierungsprüfungen werden die bei mobilen Geräten auftretenden Schwierigkeiten in zwei Kategorien unterteilt: allgemeine Probleme mit der Hardware und Software sowie Probleme hinsichtlich der Sicherheit mit dem Betriebssystem und Anwendungen. In diesem Abschnitt sehen wir uns die Probleme mit der Hardware und dem Betriebssystem näher an. Die typischen Schwierigkeiten betreffen alle Gerätekategorien und sämtliche Hersteller. In diesem Kapitel geht es um Apple iOS, Google Android und Microsoft Windows Phone. Zwar ist Windows Phone vom Markt verschwunden, es kommt in den Prüfungen jedoch noch vor und es gibt noch alte Geräte, die in Betrieb sind. Sie sollten es also für den Fall kennen, dass es Ihnen in der Praxis begegnet.

Wichtig

Für die meisten Smartphones und Tablets gibt es keine austauschbaren Ersatzteile, daher sollte ein defektes Gerät normalerweise zur Reparatur in eine geeignete Werkstatt gegeben werden. Unternehmen wie iFixit (`http://www.ifixit.com`) machen manche Bauteile einer Reparatur zugänglich, allerdings in der Regel nur für wirklich versierte Techniker.

25.1.1 Werkzeuge für die Fehlerbehebung

Da die Hardware von mobilen Geräten normalerweise nicht vom Benutzer oder einem Servicetechniker repariert oder ausgetauscht werden kann, konzentriert sich die Fehlerbehebung darauf, Probleme

mit der Software auszuschließen. Die wenigen Dinge, die man ausprobieren kann, sind auf fast alle mobilen Geräte anwendbar. Am besten fängt man mit denen an, die dem Benutzer am wenigsten Unannehmlichkeiten bereiten. Manchmal können die Probleme mit diesen Werkzeugen behoben werden oder sie helfen dabei, eine Ursache auszuschließen. In einigen Fällen stellen sie die normale Funktionalität zwar wieder her, aber das Problem tritt bald wieder auf.

Die Fehlerbehebung bei mobilen Geräten verläuft zwar etwas anders als gewohnt, deshalb sollten Sie Ihre schon erworbenen Kenntnisse nicht außer Acht lassen. Verfolgen Sie die in Kapitel 1 beschriebene Strategie zur Fehlersuche und verwenden Sie die hier erläuterten Verfahren. Wenn sich die Schwierigkeiten nicht beheben lassen oder wenn Sie die Ursache eines Problems identifiziert haben, dieses aber nicht selbst lösen können, sollten Sie das Gerät einer autorisierten Reparaturwerkstatt übergeben.

Denken Sie auch daran, dass die erforderlichen Schritte vom Gerät, dem Betriebssystem und der Betriebssystemversion abhängig sind. Möglicherweise müssen Sie auf die Ressourcen des Geräte- oder Betriebssystemherstellers zurückgreifen, um die notwendigen Schritte in Erfahrung zu bringen.

Hinweis

Die meisten der beschriebenen Werkzeuge sind entweder mit dem Verlust von Daten und Einstellungen verbunden oder bergen unter entsprechenden Umständen zumindest die Gefahr, dass es zu einem Datenverlust kommt. Teilen Sie dem Benutzer mit, welche Schritte Sie zu unternehmen gedenken und welche Art von Datenverlust damit einhergehen könnte. Geben Sie dem Benutzer die Gelegenheit, die Daten zu sichern.

Tipp

Wenn Ihnen ein Smartphone oder Tablet zur Verfügung steht, sollten Sie üben, wie Sie an die Werkzeuge zur Fehlerbehebung gelangen. Es gibt eine Menge Möglichkeiten, Änderungen vorzunehmen, wie beispielsweise die Anpassung der Helligkeit, das Schließen oder Deinstallieren von Apps und viele andere. Öffnen Sie die Einstellungen des Geräts und erkunden Sie diese. Nehmen Sie jedoch keine Änderungen vor, zu denen Sie nicht ausdrücklich berechtigt sind.

Konfiguration und Einstellungen anpassen

Bei den Betriebssystemen von mobilen Geräten gibt es eine Vielzahl von Einstellungen, ebenso wie in vielen der vom Benutzer installierten Apps. Achten Sie stets auf »Probleme«, die offenbar auf eine Fehlkonfiguration zurückzuführen sind, und untersuchen Sie sie rechtzeitig, wenn sie wahrscheinlich erscheinen. Es kostet Sie nicht viel Mühe (nur etwas Zeit), die relevanten Einstellungen zu überprüfen, erspart Ihnen aber womöglich weitere Schritte, die das Sichern und Wiederherstellen der Benutzerdaten erforderlich machen.

Wenn das Problem vermutlich nicht durch eine falsche Konfiguration verursacht wird, können Sie sich die Zeit sparen und die Konfiguration gegebenenfalls in Augenschein nehmen, nachdem Sie das Gerät neu gestartet haben (siehe Abschnitt *Warmstart,* später in diesem Kapitel). Sie möchten Ihre Zeit sicher nicht mit dem Ausprobieren verschiedener Einstellungen verschwenden, wenn ein Warmstart das Problem beheben könnte. Wenn Sie glauben, dass eine Einstellung nicht korrekt ist, müssen Sie sich die vorherige Einstellung und Ihre Änderung notieren.

Laufende Apps beenden

Alle Betriebssysteme bieten mindestens eine Möglichkeit, laufende Apps zu beenden. Am gebräuchlichsten ist die Methode, die fragliche App in der Liste der laufenden Apps in eine bestimmte Richtung zu wischen. Die Funktionsweise ist jedoch eine andere wie bei klassischen Desktop-Betriebssystemen. Damit es nicht zu Missverständnissen kommt, betrachten wir in stark vereinfachter Form, was hinter den Kulissen eigentlich vor sich geht.

Auf einem klassischen Computer öffnen Sie ein Programm, wenn Sie es benötigen, und es läuft, bis es seine Aufgabe erledigt hat, abstürzt oder von Ihnen beendet wird. Da mobilen Geräten weniger Rechenleistung und Energie zur Verfügung steht, ist es nicht erwünscht, dass geöffnete Apps Ressourcen belegen und Energie verbrauchen, wenn sie nicht im Vordergrund sind oder das Gerät sogar überhaupt nicht verwendet wird. Deshalb werden laufende Programme von modernen Betriebssystemversionen verwaltet, um die Leistung und die Akkulaufzeit zu optimieren.

Durch die Art und Weise dieser Verwaltung ist es allerdings etwas unklar, was der Begriff »laufende« App genau bedeutet. Während die aktuelle App im Vordergrund wie gewohnt läuft, laufen die verschiedenen Prozesse der im Hintergrund befindlichen Apps möglicherweise weiter, wenn sie Aufgaben zu erfüllen haben, sie können jedoch auch zwischengespeichert werden, bis sie wieder in den Vordergrund kommen, oder vom Betriebssystem beendet werden, wenn es die Ressourcen für andere Apps benötigt. Bei sauber programmierten Apps erledigt das Betriebssystem diese Verwaltung normalerweise sehr gut, dennoch kann es erforderlich sein, dass Sie eine App beenden müssen, wenn sie »eingefroren« ist, nicht mehr richtig funktioniert, oder im Verdacht steht, dass sie negative Auswirkungen auf das Verhalten des Geräts hat.

Hinweis

Vor dem Beenden einer App sollten Sie daran denken, dass der Benutzer Daten verlieren könnte oder dass (je nach App) eine bestimmte Funktion nicht verfügbar ist, bis die App wieder läuft.

Bei manchen Apps laufen (absichtlich oder unabsichtlich) Hintergrundprozesse weiter, auch wenn die Bedienoberfläche nicht mehr angezeigt wird. In Android ermöglicht es der Anwendungsmanager, eine App inklusive der dazugehörigen Hintergrundprozesse zu beenden (Abbildung 25.1). In Windows Phone können Hintergrundprozesse über die Einstellungen der App selbst oder der Einstellungen für den Akku gesteuert werden. In iOS ist im Allgemeinen ein Wischen der App nach oben ausreichend.

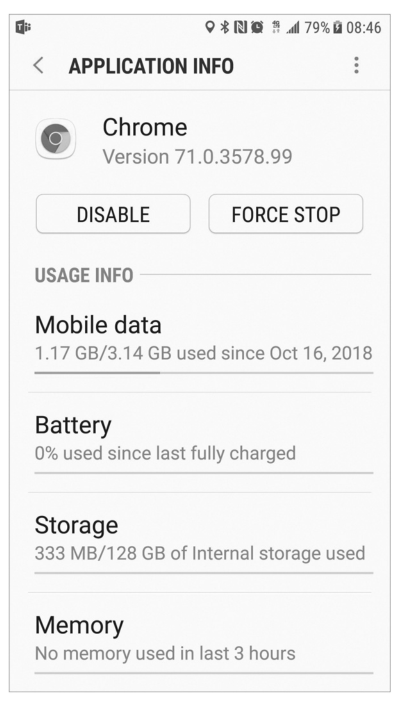


Abb. 25.1: Beenden inklusive der Hintergrundprozesse

Warmstart

Bei der Wartung von mobilen Geräten ist es wichtig, bestimmte Begriffe im Zusammenhang mit Neustarts zu kennen, insbesondere dann, wenn Sie bislang nur mit Desktop-PCs zu tun hatten. Bei einem Desktop wird ein Warmstart typischerweise vom Betriebssystem aus veranlasst oder man betätigt am eingeschalteten Gerät einen Reset-Taster. Das entscheidende Merkmal für einen Warmstart ist, dass der Rechner zu keinem Zeitpunkt komplett ausgeschaltet wird. Im Gegensatz dazu können Sie einen Kaltstart durchführen, indem Sie die Einschalttaste mehrere Sekunden lang gedrückt halten, bis der Rechner komplett ausgeschaltet ist. Das sollte zwar tunlichst vermieden werden, ist aber erforderlich, wenn das System eingefroren ist.

Bei mobilen Geräten spricht man sowohl beim Neustart vom Betriebssystem aus als auch durch das Betätigen von Hardware-Tasten von einem Warmstart. Wenn das Gerät dann immer noch nicht neustarten will, müssen Sie den Anweisungen des Herstellers folgen, um das Gerät neuzustarten. Wenn Sie wissen, wie es richtig gemacht wird, können Sie bei Geräten mit herausnehmbarem Akku das Ausschalten erzwingen, indem Sie die Abdeckung entfernen und den Akku entnehmen.

Wie bei einem Desktop-PC lassen sich viele merkwürdige Verhaltensweisen von Smartphones oder Tablets durch einen Warmstart beheben. Ich habe beim Schreiben des letzten Abschnitts beispielsweise mit Spotify auf meinem Android-Gerät Musik gehört. Als ich heute Morgen weitermachen wollte, wurde die Wiedergabe immer wieder nach wenigen Songs unterbrochen. Ich habe einen Warmstart durchgeführt, und nun ist wieder alles in Ordnung. Mehr zum Thema Warmstart im Abschnitt *Zurücksetzen auf die Werkseinstellungen*, der gleich folgt.

Apps deinstallieren und erneut installieren

Das Deinstallieren und erneute Installieren von Apps kann bei der Fehlerbehebung eine wichtige Rolle spielen. Sie können Anwendungen entweder über den App-Store deinstallieren, mit dem Sie sie installiert haben, oder aber den *Anwendungsmanager* des Geräts verwenden. Sie können sie anschließend natürlich erneut über den App-Store installieren. Wenn der Benutzer kurz nach der Installation einer App Probleme bekommt, liegt es auf der Hand, die App zu deinstallieren und zu prüfen, ob die Probleme verschwinden. Auf diese Weise können Sie ausschließen, dass die App die Probleme verursacht. Wenn die App schon genutzt wurde, sollten Sie sich vor der Deinstallation wichtige Einstellungen notieren und die Daten sichern, sofern das möglich ist.

Die Probleme, die sich durch das Deinstallieren und erneute Installieren von Apps beheben lassen, sind nicht immer so offensichtlich. Wenn ein Benutzer eine App schon länger verwendet, sie aber erst seit Kurzem Probleme bereitet, hat der Entwickler vielleicht ein fehlerhaftes Update veröffentlicht. In diesem Fall funktioniert die App möglicherweise gar nicht, arbeitet aber nach dem Deinstallieren und erneutem Installieren tadellos. In derartigen Situationen steht der Techniker womöglich schlecht da, denn was soll man tun, wenn die einzige Möglichkeit zur Behebung des Problems darin besteht, eine täglich genutzte App zu entfernen, bis der Entwickler Fehler korrigiert?

Zurücksetzen auf die Werkseinstellungen

Diese Art des Zurücksetzens löscht alle Benutzerdaten und Einstellungen und versetzt das Gerät in den Zustand, in dem es ausgeliefert wurde (zumindest die Software). Verwechseln Sie das Zurücksetzen auf die Werkseinstellungen nicht mit einem Kaltstart; wenn in der Dokumentation oder in einer Anleitung die Begriffe neustarten (reboot) und zurücksetzen (reset) synonym gebraucht werden, sollten Sie genau darauf achten, was der Autor Ihnen sagen möchte – und suchen Sie nach einer Anleitung, die nicht so schwammig ist.

Da beim Zurücksetzen auf die Werkseinstellungen sämtliche Daten und Einstellungen verloren gehen, handelt es sich hier um die gefährlichste Option, auf die Sie normalerweise nicht zugreifen werden, ohne vorher eine Sicherung der Benutzerdaten vorzunehmen (mehr dazu in Kürze). Es gibt natürlich die Ausnahme, dass Sie das Zurücksetzen auf die Werkseinstellungen absichtlich durchführen, um die Benutzerdaten zu löschen, bevor ein Gerät verkauft, recycelt oder einem neuen Benutzer übergeben wird.

Trotz der Unannehmlichkeiten ist das Zurücksetzen auf die Werkseinstellungen bei der Fehlerbehebung ein wichtiger Schritt, mit dem Sie feststellen können, ob ein Gerät einer Reparaturwerkstatt übergeben werden sollte. Falls das Zurücksetzen auf die Werkseinstellungen die Probleme behebt, diese aber nach dem Wiederherstellen der Benutzerdaten und der Programme wieder auftreten, sollten Sie die bereits erwähnten Schritte durchführen, um die App ausfindig zu machen, die Schwierigkeiten bereitet.

25.1.2 Probleme mit dem Touchscreen und der Anzeige

Zur Bedienung von mobilen Geräten wird fast ausschließlich der Touchscreen verwendet. Nur einige Geräte bieten mehr als eine Taste zum Einschalten, um mit dem Gerät zu interagieren. Probleme mit der Anzeige gehören bei allen Geräten zu den dringendsten, aber da der Touchscreen integraler Bestandteil der Bedienung von mobilen Geräten ist, gilt das hier in besonderem Maße. Im Abschnitt *Eingaben werden nicht oder nicht richtig erkannt* am Ende von Kapitel 23 haben wir bereits einige der Schritte zur Fehlerbehebung bei Touchscreens betrachtet, die Sie neben den hier genannten Schritten, die sich vornehmlich auf mobile Geräte beziehen, ebenfalls berücksichtigen sollten.

Dunkle Anzeige

Die Einstellung der Helligkeit von mobilen Geräten kann automatisch oder manuell erfolgen. Die automatische Einstellung funktioniert jedoch nicht immer zufriedenstellend. Manche Apps, die eine Einstellung der Helligkeit vornehmen, können dafür sorgen, dass die Anzeige zu hell oder zu dunkel ist.

Eine zu dunkle Anzeige kann ein Hinweis auf einen Defekt des Panels sein, aber zunächst einmal sollten Sie die Einstellungen der Anzeige überprüfen. Deaktivieren Sie die automatische Anpassung der Helligkeit, stellen Sie manuell die niedrigste und höchste Helligkeit ein und beobachten Sie, ob ein vernünftiger Helligkeitsbereich abgedeckt wird. Ist das nicht der Fall, könnte ein Defekt des Panels vorliegen. Anderenfalls könnte es sein, dass irgendetwas das richtige Funktionieren der automatischen Helligkeitsanpassung verhindert.

Die automatische Helligkeitsanpassung wird davon beeinflusst, wie viel Licht auf einen Sensor oder eine Kamera auf der Vorderseite des Geräts fällt. Vergewissern Sie sich, dass der Sensor nicht verunreinigt ist oder durch etwas anderes verdeckt wird. Falls die Anzeige in einem dunklen Raum zu hell ist, sollten Sie sich in der Umgebung nach hellen Lampen umsehen, die zwar zu weit entfernt sind, um Ihren Aufenthaltsort auszuleuchten, aber vom Sensor wahrgenommen werden, wenn er in die richtige Richtung weist.

Achten Sie auch auf Apps, die Änderungen an der Helligkeit des Geräts vornehmen. Möglicherweise verwendet eine App eigene Helligkeitseinstellungen, die Änderung der Helligkeit kann aber auch systemweit erfolgen. Apps zum Lesen von E-Books, wie Amazon Kindle, sind ein Beispiel hierfür. Probieren Sie aus, ob die Anzeige nach einem Warmstart wieder richtig funktioniert, und prüfen Sie, ob das Problem erneut auftritt, wenn Sie die fragliche App erneut verwenden. Hin und wieder gerät die Kindle-App auf meinem Android-Gerät mit der automatischen Helligkeitsanpassung in Konflikt, was zu merkwürdigen Änderungen der Helligkeit führt, bis ich einen Warmstart des Tablets durchführe. In diesem Fall besteht die Lösung wohl einfach darin, den Benutzer zu bitten, einen Warmstart durchzuführen, wenn solche Apps derartige Probleme verursachen.

Touchscreen reagiert nicht

Wenn der Touchscreen nicht oder nicht richtig reagiert, kann es hierfür verschiedene einfache Ursachen geben: Verunreinigungen, unbeabsichtigte Berührungen oder Probleme mit der Leistung. Wenn diese möglichen Ursachen beseitigt sind, müssen wir mit schlimmeren Gründen rechnen.

Unbeabsichtigte Berührungen Dieses Problem lässt sich am einfachsten beheben. Manchmal hält ein Benutzer das Gerät so, dass der Touchscreen einen Teil des Arms oder der Hand als eine Berührung erkennt und eventuell überhaupt nicht auf beabsichtigte Berührungen reagiert. Überempfindli-

che Sensoren und schlechtes Design können das Problem verschärfen, aber die Lösung ist stets dieselbe: Zeigen Sie dem Benutzer, wieso der Sensor unabsichtliche Berührungen erkennt, und erklären Sie, wie man das Gerät halten muss, um sie zu vermeiden.

Verunreinigter Bildschirm Auch das Problem eines verunreinigten Bildschirms lässt sich leicht lösen. Meistens reicht es schon aus, den Bildschirm mit einem trockenen Mikrofasertuch abzuwischen und ihn dadurch von Fingerabdrücken, Staub und sonstigen Verunreinigungen zu befreien (Abbildung 25.2).

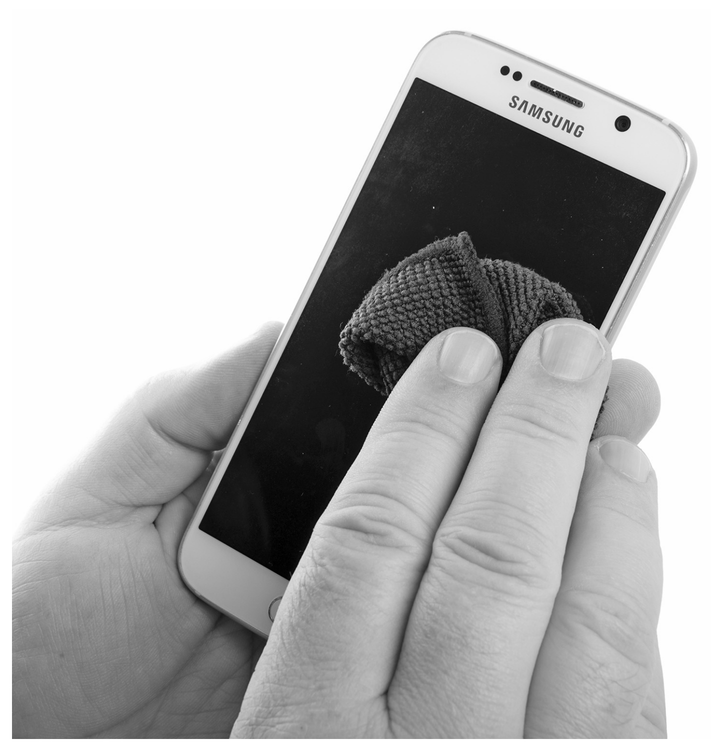


Abb. 25.2: Reinigen eines Smartphones

Probleme mit der Leistung Wenn ein normaler PC Probleme mit der Leistung hat, kann der Mauszeiger einfrieren oder wild auf dem Bildschirm herumspringen. Bei einem Smartphone oder Tablet scheint der Touchscreen bei Problemen mit der Leistung überhaupt nicht mehr oder fehlerhaft und ungenau zu reagieren. Haben Sie Geduld mit dem Gerät und suchen Sie nach Hinweisen, ob es überlastet ist. Wird die richtige Uhrzeit angezeigt? Laufen gegebenenfalls vorhandene Animationen des Sperrbildschirms oder des Bildschirmschoners flüssig ab?

Werden die Widgets für Wettervorhersage oder Aktienkurse auf dem Sperrbildschirm aktualisiert, wenn die Netzverbindung zu funktionieren scheint? Reagiert das Gerät nur langsam, wenn Sie Hardware-Tasten betätigen? Überprüfen Sie, ob das Gerät Textnachrichten empfangen kann und ob Anrufe funktionieren. Wenn die Probleme offenbar mit der Leistung zusammenhängen, sollten Sie einen Warmstart durchführen und testen, ob der Touchscreen wieder funktioniert.

Viele Benutzer verwenden Schutzfolien, um den Bildschirm ihrer Geräte vor Kratzern zu bewahren. Eine nicht ordnungsgemäß angebrachte Schutzfolie kann dazu führen, dass der Touchscreen nicht richtig funktioniert. Überprüfen Sie die Anweisungen des Herstellers und entfernen und ersetzen Sie eine nicht ordnungsgemäß angebrachte Schutzfolie.

Kalibrierung und Diagnose

Wenn der Touchscreen auch nach einem Warmstart nicht funktioniert, sollten Sie online recherchieren, ob das Gerät über ein verborgenes Diagnosemenü verfügt. Um es anzuzeigen, muss meist eine bestimmte Ziffernfolge auf der Telefontastatur eingegeben werden oder Sie müssen nach einem Warmstart bestimmte Tasten gedrückt halten, während das Gerät startet. Falls das Gerät über ein Diagnosewerkzeug für den Touchscreen verfügt, sollten Sie mit seiner Hilfe in der Lage sein, zu beurteilen, ob der Touchscreen noch funktioniert. Einige Android- oder Windows-Phone-Geräte bieten entweder über die Systemeinstellungen oder in Form eines verborgenen Menüs die Möglichkeit, den Touchscreen zu kalibrieren.

Physische Beschädigung

In Kapitel 23 habe ich Beschädigungen von tragbaren Computern erläutert, aber bei mobilen Geräten können Probleme auftreten, die bei größeren Geräten selten sind. Schon ein kurzes Eintauchen in der Toilette, im Swimmingpool oder in einem Glas Margarita kann einem Gerät den Garaus machen. Wenn ein Gerät feucht wird oder auf eine harte Oberfläche stürzt, kann das zu ernsthaften Problemen führen. Wenn man bei einem heftigen Regenschauer ein Smartphone in der Hosentasche hat oder ein Gerät auf dem Tisch liegt, wenn jemand ein Getränk verschüttet, kann das dazu führen, dass Flüssigkeit in die kleinsten Ecken und Winkel des Geräts vordringt.

Manche Geräte verkraften etwas Feuchtigkeit, viele sind aber völlig ungeschützt gegen ein Eintauchen in Flüssigkeiten. Wenn ein Smartphone in die Toilette fällt, kann das einem wirklich den Tag verderben. Wenn der Akku nicht entnehmbar ist, kann man tatsächlich nicht viel tun, um ein flüssigkeitsdurchtränktes Smartphone oder Tablet zu retten.

Wenn Sie die einfachsten Erklärungen ausschließen können und die Tipps zur Fehlerbehebung nicht weiterhelfen, ist es an der Zeit, nach Hinweisen darauf zu suchen, ob das Gerät nass geworden oder gefallen ist. Hierfür gibt es eine altmodische Methode: Fragen Sie den Benutzer. Dabei müssen Sie sich natürlich darüber im Klaren sein, dass niemand gerne zugibt, dass ein Smartphone nicht mehr funktioniert, nachdem er es vor Lachen prustend mit Milch besprüht hat, weil er beim Frühstück XKCD gelesen hat.

Tipp

Sehen Sie sich die Comics auf `http://xkcd.org` an. Humor für Nerds vom Feinsten!

Auch wenn das Glas keine Sprünge zeigt, könnten durch den Sturz interne Leitungen beschädigt worden sein. Feuchtigkeit kann zu internen Kurzschlüssen führen, und verbliebene Flüssigkeit kann für ein wirklich seltsames Verhalten der Sensoren sorgen. Die meisten Geräte enthalten einige Flüssigkeitskontaktindikatoren (*Liquid Contact Indicator*, LCI), die ihre Farbe dauerhaft ändern, wenn sie mit einer Flüssigkeit in Berührung gekommen sind (Abbildung 25.3). Sie dienen vor allem dazu, dass der Hersteller Garantieleistungen bei durch Wasser verursachten Schäden verweigern kann. Wo diese Indikatoren jeweils angebracht sind, können Sie online recherchieren. Häufig befinden sich im Akkufach oder auf dem Akku selbst solche Indikatoren, die für gewöhnlich weiß sind, sofern sie noch nicht nass geworden sind.

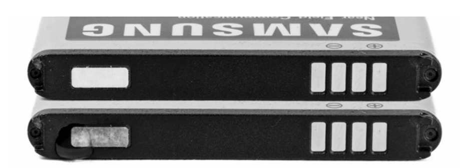


Abb. 25.3: Der obere Flüssigkeitskontaktindikator ist intakt, der untere ist mit einem Wassertropfen in Berührung gekommen.

25.1.3 Eine App startet nicht

Es kann verschiedene Gründe dafür geben, dass eine App nicht startet oder sich nicht richtig installieren lässt. Zunächst einmal könnte es sein, dass die App für bestimmte Kombinationen aus Betriebssystemversion, Hardware und herstellerspezifischen Anpassungen des Betriebssystems Ihres Geräts nicht geeignet ist. Bei Android-Geräten besteht beispielsweise die Möglichkeit, dass die auf dem Gerät installierte Android-Variante nicht mit der App kompatibel ist, weil die verschiedenen Hersteller nach eigenem Gutdünken Änderungen am Betriebssystem vornehmen – und das kann zu Kompatibilitätsproblemen mit den Apps anderer Hersteller führen.

Ein weiterer Grund dafür, dass eine App nicht startet, könnte sein, dass ein Gerät die typischen Anforderungen an die Hardware nicht erfüllt, wie beispielsweise verfügbarer Arbeitsspeicher, Speicherplatz oder Prozessortyp, oder aber dass ein bestimmter Sensor fehlt oder Fähigkeiten der Kamera benötigt werden, die diese nicht unterstützt. Vor der Installation eines Programms oder wenn es Probleme bereitet, sollten Sie immer einen Blick auf die Systemanforderungen einer App werfen.

Sowohl iOS- als auch Android-Geräte zeichnen von Anwendungen verursachte Fehler auf. Zum Auslesen dieser Protokolle benötigen Sie die Entwicklertools von Apple oder bei Android-Software von Drittherstellern. Das sollten Sie sich merken, für den Fall, dass ein anderer Techniker oder ein App-Programmierer (falls unternehmenseigene Apps entwickelt werden) Hilfe bei der Fehlersuche braucht.

25.1.4 Überhitzung

Ebenso wie die in Kapitel 23 erörterten tragbaren Computer können auch mobile Geräte durch Überhitzung Schaden nehmen. Die meisten der dortigen Ratschläge sind auch für mobile Geräte gültig. Allerdings haben wir insbesondere zu Smartphones ein anderes Verhältnis. Sie sind fast immer eingeschaltet, wir haben sie ständig in der Hand oder zumindest in der Hosen- oder Jackentasche und wir nehmen sie an Orte mit, bei denen uns nicht einmal im Traum einfallen würde, sie mit einem Laptop aufzusuchen. Zudem ist es wahrscheinlicher, ein mobiles Gerät an einem heißen Sommertag auf dem Beifahrersitz liegen zu lassen oder es im Winter gut geschützt unter der isolierenden Kleidung in Körpernähe zu tragen.

Zu einer Überhitzung kann es durch die Kombination verschiedener Faktoren kommen: durch die vom Gerät selbst erzeugte Wärme, durch externe Wärmequellen, wie etwa Sonneneinstrahlung oder eine Lampe, und durch eine Umgebung, in der die Wärme erhalten bleibt, weil sie nur schlecht abgeführt werden kann. Da wir die Geräte so häufig benutzen, haben wir des Öfteren die Gelegenheit, zu bemerken, was normal ist und was nicht. Wenn ein Gerät heiß ist, sollten Sie die drei genannten Faktoren überprüfen und sich fragen, ob sie die hohe Temperatur des Geräts erklären können. Die Suche nach einer vernünftigen Erklärung kann dabei helfen, Probleme mit der Leistung ausfindig zu machen, bevor der Akku entleert wird, verhindert Beschädigung von Bauteilen durch die Hitze und ermöglicht es, Probleme mit dem Akku oder der Stromversorgung zu entdecken, bevor sie gefährlich werden.

Laden des Akkus, große Datentransfers, eingefrorene Apps, Aufzeichnung von hochauflösenden Videos und andere belastende Aufgaben können dafür sorgen, dass ein Gerät sehr viel heißer wird als sonst. Vermeiden Sie es, ein Gerät belastende Aufgaben an heißen und wärmeisolierten Orten ausführen zu lassen. Nehmen Sie die Geräte nicht an sehr heiße Orte mit, wenn es sich vermeiden lässt. Sollte das nicht möglich sein, schalten Sie das Gerät am besten aus, um das Risiko zu minimieren. Wenn sich das Gerät in einer kühlen Umgebung sehr heiß anfühlt, sollten Sie es in den Flugmodus versetzen, alle laufenden Apps beenden und prüfen, ob es abkühlt. Ist das nicht der Fall, sollten Sie es ausschalten und abwarten, bis es abgekühlt ist. Versuchen Sie es anschließend erneut.

Die größten Sorgen muss man sich bei Geräten machen, die ohne ersichtlichen Grund von allein überhitzen oder so heiß werden, dass man sich daran verbrennen kann. Dabei handelt es sich fast immer um ein Hardware-Problem, wie z.B. ein defekter Akku oder ein defekter Schaltkreis im Inneren des Geräts. Hier kann man nichts ausrichten – schalten Sie das Gerät aus, um es vor weiteren Schäden zu bewahren, und geben Sie es in eine Reparaturwerkstatt.

Wenn das Problem der Überhitzung nicht in Angriff genommen wird, selbst wenn sie aus eigentlich harmlosen Gründen erfolgt, läuft man Gefahr, dass das Gerät Schaden nimmt und Daten verloren gehen. Schlimmstenfalls überhitzt es so sehr, dass es zu einem Sicherheitsrisiko wird und beim Anfassen Verbrennungen verursacht und Stromschläge austeilt oder dass ein aufgeplatzter Akku einen Brand verursacht oder sogar explodiert.

25.1.5 Mangelnde Geschwindigkeit

Mobile Geräte können ebenso wie Desktop-PCs und Laptops unter Performanceproblemen leiden, oft aus denselben Gründen. Sie können durch nahezu ausgelastete Speichergeräte verursacht werden, die es unmöglich machen, Daten zu speichern oder Apps zu installieren. Darüber hinaus können die Geräte davon betroffen sein, dass zu viele Apps gleichzeitig ausgeführt werden, die den Arbeitsspeicher belegen.

Im Betriebssystem gibt es meist eine Einstellung, die es ermöglicht, solche Apps zu beenden oder ihren Ressourcenbedarf anzuzeigen, insbesondere den belegten Arbeitsspeicher und den erforderlichen Speicherplatz. Wenn der Speicherplatz zu knapp ist, müssen Sie womöglich einige Apps entfernen oder sie auf einem Wechseldatenträger wie Micro- oder Mini-USB-Speicherkarte neu installieren.

Ein Gerät mit Performanceproblemen wird oft sehr warm – das ist ein deutlicher Hinweis. Befolgen Sie die Ratschläge aus dem letzten Abschnitt, um zu beurteilen, ob das Gerät oder die Umgebung die Ursache für die Überhitzung ist. Ein heiß gelaufenes Gerät könnte die Taktfrequenz drosseln, um die CPU vor Überhitzung zu schützen, indem die Leistung reduziert wird. In diesem Fall sollte die Leistung wieder zunehmen, sobald das Gerät abgekühlt ist.

Einer der ersten Schritte bei der Behebung von Geschwindigkeitsproblemen ist ein Warmstart des Geräts. Dadurch werden alle aktiven Apps aus dem Arbeitsspeicher entfernt – auch solche, die abgestürzt sind oder nicht korrekt arbeiten. Was die Fehlersuche betrifft: Zum Ermitteln der Leistungsdaten können Sie die Geräteeinstellungen oder Apps von Drittanbietern verwenden. Manchmal können solche Apps dabei helfen herauszufinden, wodurch die Probleme verursacht werden. Wenn Sie am Ende zu dem Schluss kommen, dass ein Hardware-Problem für die mangelnde Geschwindigkeit verantwortlich ist, sollten Sie das Gerät zu einer autorisierten Reparaturwerkstatt bringen.

25.1.6 Akkulaufzeit

Die aktuellen Geräte verwenden, wie die in Kapitel 23 erörterten tragbaren Computer, Li-Ion-Akkus (Lithium-Ionen). Normale Laptops lassen sich meist auch während des Ladens relativ einfach benutzen. Die Ergonomie von mobilen Geräten macht es hingegen schwierig, sie während des Ladevorgangs zu verwenden. Umso wichtiger ist es, zu gewährleisten, dass genügend Akkukapazität verfügbar ist, wenn sie benötigt wird. Wir sehen uns an, wie man mit Akkus umgehen sollte, um ihre Leistung bestmöglich zu nutzen. Aber zunächst einmal komme ich zu den Grundlagen der Energieverwaltung.

Energiebedarf

Die Akkus verschiedener mobiler Geräte unterscheiden sich deutlich hinsichtlich der Laufzeit bei normaler Nutzung, dem zeitlichen Abstand zwischen zwei Ladezyklen und der elektrischen Leistung, die sie liefern können bzw. die zum Aufladen erforderlich ist. Sie sollten gewährleisten, dass mobile Geräte über eine hinreichend lange Akkulaufzeit verfügen, um über einen angemessenen Zeitraum hinweg eine »normale« Nutzung zu ermöglichen.

Die von den Herstellern genannten Akkulaufzeiten sind ein guter Hinweis, man sollte die Angaben allerdings mit Vorsicht genießen. Auf verschiedene Websites sind Tests der verbreiteteren Geräte zu finden. Dort können Sie nachlesen, wie lange ein Gerät bei einer bestimmten energiehungrigen Aufgabe durchhält, beispielsweise bei der Wiedergabe von hochauflösenden Videos. Bringen Sie in Erfahrung, wie lange das Gerät eines Benutzers mit einer Ladung durchhalten muss, und versuchen Sie, ein Gerät bereitzustellen, das mindestens 20 Prozent länger durchhält, um der allmählich nachlassenden Akkukapazität Rechnung zu tragen.

Sollte es kein Gerät geben, das den Anforderungen des Benutzers gerecht wird, können Sie dem Benutzer ein Gerät mit entnehmbarem Akku nebst Ersatzakku oder aber ein tragbares Ladegerät bereitstellen. Sie können ein Smartphone oder ein Tablet unterwegs mit einer sogenannten *Powerbank* aufladen, wenn keine Steckdose verfügbar ist.

Energieverwaltung

Bei der Akkulaufzeit sind vor allem zwei Punkte zu beachten, nämlich wie lange ein Akku mit einer Ladung durchhält und wie lange er Ihren Ansprüchen gerecht wird, bis er durch einen neuen Akku ersetzt werden muss. Erfreulicherweise ist hier eine gleichzeitige Optimierung möglich. Wenn Sie Energie für Leistungsmerkmale vergeuden, die gar nicht benutzt werden, muss das Gerät nicht nur öfter als nötig geladen werden, die zusätzlichen Ladezyklen verkürzen auch die Lebensdauer des Akkus. Sehen wir uns also einmal an, wodurch am meisten Energie verbraucht wird. Schenken Sie aber auch der Anzeige des Energieverbrauchs auf Ihrem Gerät Beachtung, um zu ermitteln, wodurch am meisten Energie verbraucht wird.

Anzeige Der Energieverbrauch hängt in gewissem Maße von der Größe und Art des Bildschirms ab, aber am schnellsten wird der Akku geleert, wenn der Bildschirm ständig eingeschaltet ist. Schalten Sie ihn aus, falls möglich, und verwenden Sie die niedrigste noch akzeptable Einstellung für die Helligkeit. Weil die Anzeige bei voller Helligkeit so viel besser aussieht, ist das oftmals die Voreinstellung. Die Energieeinsparung bei niedriger Helligkeit ist zwar verlockend, aber der beste Kompromiss ist im Allgemeinen die automatische Einstellung der Helligkeit. Abbildung 25.4 zeigt den Energieverbrauch. Beachten Sie, wie viel Energie allein der eingeschaltete Bildschirm verbraucht!



Abb. 25.4: Energieverbrauch eines Smartphones

Es gibt weitere Möglichkeiten, den Energieverbrauch des Bildschirms zu optimieren, die sich jedoch von Hersteller zu Hersteller unterscheiden. Üblicherweise können Sie einstellen, wie lange der Bildschirm eingeschaltet bleibt, wenn Sie keine Eingaben vornehmen, und ob der Bildschirm eingeschaltet wird, wenn Sie eine Nachricht erhalten. Einige Geräte verfügen über einen *Stromsparmodus* und sind möglicherweise sogar in der Lage, anstatt einer farbigen Darstellung Graustufen zu verwenden, um Energie zu sparen. OLED-Bildschirme benötigen weniger Energie, um dunkle Farben darzustellen. Wenn Ihr Gerät ein OLED-Panel besitzt, können Sie den Energieverbrauch senken, indem Sie einen dunklen Bildschirmhintergrund verwenden und für Apps ein dunkles Erscheinungsbild konfigurieren (sofern verfügbar).

Drahtlose Kommunikation Für die Akkulaufzeit spielt die Nutzung des Netzwerks eine entscheidende Rolle. Sie sollten stets daran denken, dass jede Form der drahtlosen Kommunikation (Telefonie, Mobilfunkdaten, WLAN, Bluetooth, NFC etc.) einen Sender/Empfänger im Gerät erfordert. Sobald ein Gerät eines der Kommunikationsverfahren nutzt, ist der entsprechende Sender/Empfänger aktiv und verbraucht Energie. Selbst wenn Sie gar keine Daten übertragen, wird dadurch Energie verbraucht – und das kann die Akkulaufzeit erheblich verkürzen. Der Energieverbrauch ist von der Kommunikationsmethode und den genauen Umständen abhängig, aber hier sind zwei Faustregeln: Die Suche nach Signalen benötigt viel Energie, und die Apps auf einem Gerät sind häufiger im Hintergrund aktiv, wenn Verbindungen verfügbar sind.

Wenn man auf Reisen ist, versuchen mobile Geräte insbesondere in dünn besiedelten Gebieten ständig, das beste Funksignal zu finden. Auch diese Suche nach Netzwerken kann die Laufzeit des Akkus deutlich senken. Dieser ungewollte Energieverbrauch lässt sich bei den meisten Geräten allerdings verhindern, indem man in den Systemeinstellungen konfiguriert, weniger oft nach Mobilfunkzellen oder drahtlosen Netzwerken zu suchen. Eine weitere Möglichkeit ist es, die verschiedenen Kommunikationstechnologien zu deaktivieren, wenn sie nicht benötigt werden. Sie möchten sicherlich nicht auf einer abgelegenen Landstraße in einer Schneewehe stecken bleiben, nur um dann feststellen zu müssen, dass der Akku durch die permanente Suche nach Mobilfunksignalen fast vollständig entladen ist.

Auch wenn eine Verbindung stabil ist, wird kontinuierlich Energie verbraucht, um Daten zu senden und zu empfangen. Man nimmt dieses langsame Entladen oft in Kauf, weil man möchte, dass die Verbindung zur Verfügung steht. Denken Sie jedoch daran, dass manche Apps nur wenig Energie benötigen, wenn keine Verbindung besteht, aber bei verfügbarer Verbindung im Hintergrund viele Aufgaben erledigen, die Energie verbrauchen. Am einfachsten ist es, die Verbindungen zu deaktivieren, aber das Betriebssystem (und in manchen Fällen die App selbst) bietet die Möglichkeit, einzustellen, wann eine App Daten im Hintergrund senden und empfangen und welche Verbindungen sie verwenden darf.

Ortungsdienste Grundsätzlich gelten für die dauerhafte Nutzung von GPS oder Ortungsdiensten sehr ähnliche Regeln, es gibt jedoch einige erwähnenswerte Unterschiede. Wenn die Ortungsdienste aktiv sind, können Apps die Position des Geräts abfragen. Je nachdem, wie Sie das Gerät konfiguriert haben, erfolgt die Ermittlung der Position durch energiesparende (ungenauere) Verfahren, etwa mithilfe von Mobilfunknetzen oder WLANs in der Umgebung, durch sehr genaue (aber energiehungrige) Verfahren, wie GPS, oder durch eine Kombination dieser Verfahren. Dabei kann es sich um Apps handeln, die im Hintergrund arbeiten oder um im Vordergrund laufende Apps, wie Navigationssoftware, die auf den GPS-Empfänger zugreift. Der Energieverbrauch kann hier stark schwanken, je nachdem, ob eine App gelegentlich im Hintergrund eine ungenaue Positionsabfrage durchführt oder kontinuierlich eine genaue Aktualisierung der Position abfragt.

Die einfachste Lösung für dieses Problem ist, Ortungsdienste abzuschalten, wenn sie nicht benötigt werden. Vielleicht finden Sie auch einen sinnvollen Kompromiss, indem Sie die Einstellungen der Apps, die auf Ortungsdienste zugreifen, konfigurieren. Falls eine App Ortungsdienste benötigt (z.B. Apps, die Restaurants oder Kinos in der näheren Umgebung anzeigen oder speziellere Apps, die zum Geocaching, zum Navigieren oder zur Anzeige von Landkarten dienen), diese aber nicht verfügbar sind, werden Sie aufgefordert, die Ortungsdienste zu aktivieren.

Weil Apps, für die eine Ortsbestimmung nicht so wichtig ist, sich auch mit veralteten Positionsdaten zufriedengeben, hängt ein sinnvoller Kompromiss letztlich davon ab, wie Sie Ihr Gerät nutzen und

welche Apps Sie verwenden. Wenn Sie Ihr Gerät regelmäßig dazu verwenden, Fotos von Graffiti oder von Schlaglöchern inklusive Ortsangaben aufzunehmen, möchten Sie sicherlich immer möglichst genaue Positionsdaten verwenden, ohne auf die Akkulaufzeit zu achten. Eine weitere Möglichkeit ist es, die Konfiguration von Apps zu überprüfen, die Ortungsdienste verwenden, und diejenigen zu deaktivieren, die keine aktuellen Positionsdaten benötigen.

Wichtig

Die verschiedenen Faktoren, die Einfluss auf die Akkulaufzeit und die Lebensdauer des Akkus haben, sollten Sie kennen.

25.1.7 Aufgequollener Akku

Aus Kapitel 23 wissen Sie, dass es bei den Akkus von mobilen Geräten das Phänomen gibt, dass diese unter ungünstigen Umständen aufquellen können. Der häufigste Grund ist eine Überladung, die stattfindet, wenn die Schaltkreise defekt sind, die das eigentlich verhindern sollen. Die Verwendung unpassender Ladegeräte oder ungeeigneter Akkus, die nicht die erforderlichen Werte für Spannung und Leistung besitzen, stellen ein weiteres Risiko dar, ebenso wie eine Überhitzung. In manchen Fällen ist der Akku einfach nur defekt.

Vorsicht

Versuchen Sie unter keinen Umständen, einen Akku zu reparieren, schon gar nicht, wenn er aufgequollen ist, denn Sie könnten sich dabei verletzen oder das Gerät beschädigen.

Vorbeugen ist besser als heilen. Lassen Sie Akkus nicht überhitzen, insbesondere nicht beim Laden. Verwenden Sie vorzugsweise Ladegeräte und Akkus des Geräteherstellers. Suchen Sie in der Dokumentation des Herstellers nach Hinweisen, was man tun und lassen sollte. Auch eine Vorbeugung bietet keinen vollständigen Schutz. Aufgequollene Akkus können platzen, gefährliche Flüssigkeiten absondern und Feuer fangen. Sie müssen sich darüber im Klaren sein, dass so etwas passieren kann. Seien Sie wachsam und achten Sie auf Hinweise darauf, und seien Sie vorsichtig bei der Entsorgung aufgequollener Akkus.

Halten Sie auch nach weniger deutlichen Hinweisen Ausschau. Schließen Geräterahmen und Bildschirm bündig ab? Liegt das Gerät auf einer glatten Oberfläche plan? Ist die Rückseite des Geräts gewölbt? Gibt es knarzende oder knarrende Geräusche von sich? Wird es ohne ersichtlichen Grund heiß? Wenn das Gerät über eine abnehmbare Abdeckung verfügt, ist es ganz einfach, den Akku zu überprüfen. Wenn das nicht der Fall ist, sollten Sie eine Reparaturwerkstatt aufsuchen oder einen Servicetechniker beauftragen, um das Gerät zu überprüfen.

Wenn Sie es mit einem aufgequollenen Akku zu tun bekommen, gibt es wirklich keine andere Möglichkeit, als ihn, wie im Kasten *Recycling alter Akkus* in Kapitel 23 beschrieben, zu entsorgen und ihn zu ersetzen, vorzugsweise durch ein Markenprodukt des Computerherstellers.

Wichtig

Giftige Bauteile, wie Akkus von Smartphones, Tablets oder Handys, müssen sachgerecht entsorgt oder recycelt werden. Das gilt auch für die Geräte selbst. Geben Sie sie bei der entsprechenden Sammelstelle ab. Die Entsorgung über den Hausmüll ist Umweltverschmutzung und schadet uns allen.

25.1.8 Systemstillstand

Ein Smartphone oder Tablet kann – ebenso wie normaler PC – einfrieren (und zwar aus den gleichen Gründen). Die Unterschiede zwischen den Betriebssystemen und die verschiedenen Eingabemetho-

den bedeuten jedoch, dass es bei mobilen Geräten weniger Möglichkeiten gibt, einen solchen Absturz des Gerät zu handhaben. Das unmittelbare Ziel ist, das Geräts wieder in einen brauchbaren Zustand zu versetzen. Wenn es nicht mehr reagiert, müssen Sie einen Warmstart durchführen. Ohne Zugriff auf das Betriebssystem müssen Sie der Anleitung des Herstellers folgen, um einen Warmstart durchzuführen. In den meisten Fällen müssen Sie die Einschalttaste ein paar Sekunden lang gedrückt halten oder den Akku entfernen.

Hinweis

Wenn ein Gerät offenbar eingefroren zu sein scheint, besteht auch die Möglichkeit, dass nur der Touchscreen nicht mehr korrekt funktioniert. Prüfen Sie, ob das Gerät auf das Betätigen von Hardware-Tasten oder auf Sprachbefehle normal reagiert, bevor Sie davon ausgehen, dass es abgestürzt ist.

Wenn das Gerät zumindest teilweise noch reagiert, können Sie versuchen, einen möglicherweise für die Probleme verantwortlichen Prozess in der Liste der laufenden Anwendungen zu beenden. Aber auch nach dem Beenden können die Probleme erneut auftreten, sobald die App wieder geöffnet wird. Verschwenden Sie besser keine Zeit und schließen Sie die problematische App, sichern Sie die Daten anderer laufender Apps und führen Sie einen Warmstart durch.

Wenn das Gerät wieder läuft, können weitere Schritte erforderlich sein. Wenn Sie wissen, dass das Gerät beim Öffnen einer neuen oder aktualisierten App abgestürzt ist, müssen Sie die App deinstallieren und auf eine Aktualisierung warten – oder sich nach Ersatz umsehen. Manchmal ist auch das Betriebssystem selbst für Abstürze verantwortlich, insbesondere nach einer Aktualisierung. Achten Sie also auf Patches, die diese Art von Problemen beheben. Wenn das Gerät zu beliebigen Zeitpunkten und immer öfter plötzlich einfriert, wenn es bestimmte Aufgaben ausführt (wie beispielsweise Zugriff auf Apps, die GPS oder die Kamera verwenden), handelt es sich vermutlich um ein Hardware-Problem und das Gerät muss repariert werden.

Es kann auch vorkommen, dass ein Gerät nach einem Warmstart noch immer unbrauchbar ist. In diesem Fall müssen Sie in der Dokumentation des Herstellers nachlesen, wie man es in einen speziellen Modus versetzt, in dem die problematische App gelöscht, die Betriebssysteminstallation repariert oder das Gerät auf die Werkseinstellungen zurückgesetzt werden kann. Wenn auch diese Vorgehensweise keine Abhilfe schafft, werden Sie das Gerät wohl in eine Reparaturwerkstatt geben müssen.

25.1.9 Keine Bildausgabe auf externem Monitor

In Kapitel 24 haben Sie erfahren, dass viele mobile Geräte einen Videoausgang besitzen, um Inhalte auf einem externen Monitor oder über einen Projektor wiederzugeben. Wenn man es richtig anstellt, funktioniert das fast von allein: Schließen Sie einen Adapter an Ihr mobiles Gerät an und verbinden Sie dann den Adapter mit dem VGA-, DVI-, DP- oder HDMI-Eingang des Monitors – schon haben Sie ein Bild.

Nun ja, zumindest theoretisch. In der Praxis ist die Darstellung der Inhalte auf externen Monitoren oft problematisch. Die auftretenden Schwierigkeiten hängen zwar auch vom Gerätetyp ab, aber hier sind einige wohlerprobte Tipps, wenn die Bildausgabe auf einem externen Monitor nicht klappen will:

- Ist die Bildeingangsquelle beim externen Ausgabegerät richtig eingestellt? Fast alle Monitore, TVs und Projektoren besitzen mehrere Eingänge und die Eingangsquelle muss natürlich korrekt eingestellt sein.
- Haben Sie den passenden Adapter für Ihr Gerät? Allein Apple hat in den vergangenen paar Jahren fünf verschiedene Arten von Videoadaptern herausgebracht – und von den ganzen Adaptern für Android-Geräte will ich gar nicht erst anfangen! Vergewissern Sie sich also, ob Sie einen für Ihr Gerät geeigneten Adapter verwenden.
- Benötigt der Adapter eine eigene Stromversorgung?

- Falls Sie HDMI benutzen: Hat der Monitor Ihr Gerät erkannt und umgekehrt? Je nach Hersteller und Modell kann es erforderlich sein, dass Monitor und/oder Videoquelle zurückgesetzt werden müssen, damit HDMI die verbundenen Geräte erkennt.

25.1.10 Keine Tonausgabe

Probleme mit der Tonausgabe treten bei mobilen Geräten ebenfalls oft auf. Der wohl häufigste Fehler besteht darin, dass die Lautstärke durch die Systemeinstellungen oder eine App heruntergeregelt ist oder dass die Lautsprecher auf stumm geschaltet sind. Dieser Fehler lässt sich im Prinzip leicht beheben, aber unter Umständen muss man eine ganze Reihe von Einstellungen durchgehen, bis man herausgefunden hat, welche App oder Konfiguration die Lautsprecher schweigen lässt. Manche Geräte verwenden verschiedene Lautstärkeeinstellungen für die Wiedergabe von Medien, Telefongesprächen, Benachrichtigungen und anderes. Da kann es leicht passieren, dass man die falsche ändert.

Einige mobile Geräte besitzen Hardware-Tasten zum Einstellen der Lautstärke. Überprüfen Sie das gegebenenfalls. Wenn das nicht funktioniert, müssen Sie der Reihe nach die Einstellungen des Geräts und der Apps überprüfen. Wenn Sie partout nicht weiterkommen, liegt vermutlich ein Hardware-Problem vor. Beispielsweise könnten sich die Lautsprecherkabel im Inneren des Geräts gelöst haben oder die Lautsprecher selbst sind defekt. Wie immer in solchen Fällen werden Sie das Gerät wohl in eine Reparaturwerkstatt geben müssen.

25.1.11 Verbindungsprobleme

Allgemeine Probleme mit Netzwerkverbindungen, die alle Geräte betreffen, wurden bereits an anderer Stelle in diesem Buch erörtert. Bei mobilen Geräten gibt es jedoch einige weitere Verbindungsprobleme zu beachten, die Ihnen wahrscheinlich früher oder später begegnen werden. Wir werden auch Mobilfunksignale betrachten, aber das erste Problem betrifft WLAN- und Bluetooth-Verbindungen. Größtenteils lassen sich diese Verbindungsprobleme unmittelbar beheben. Aber irgendwann werden Sie unweigerlich feststellen, dass ein Verbindungsproblem Schwierigkeiten bereitet, oder zumindest ausschließen wollen, dass ein Verbindungsproblem die eigentliche Ursache der Schwierigkeiten ist.

Das offensichtlichste Problem, unter dem mobile Geräte leiden, sind schwache Signale. Ein schwaches Signal kann verschiedene Ursachen haben. Vielleicht befinden Sie sich weit im Inneren eines großen Gebäudes, in einer tiefen Schlucht zwischen mehreren Wolkenkratzern, im Niemandsland zwischen weit entfernten Funkzellen in dünn besiedelten Gebieten oder in einer anderen von vielen vergleichbaren Situationen. Die typischen Symptome für ein schwaches Signal sind unterbrochene Verbindungen, Verzögerungen, niedrige Datenübertragungsraten und die häufige Anzeige, dass das Gerät nach einem Signal sucht.

Gegen ein schwaches Signal kann man kaum etwas ausrichten, außer es im Auge zu behalten. Es werden zwar Signalverstärker angeboten, die aber von zweifelhaftem Nutzen sind. Sie funktionieren am besten, wenn man sich an einem festen Ort befindet, der weit von der Funkzelle entfernt ist. Wenn sich der Benutzer in Bewegung befindet, sind sie für gewöhnlich nutzlos.

Hinweis

Neben einem schwachen Signal können auch Performanceprobleme auf dem Gerät selbst die Symptome einer geringen Datenübertragungsrate einer Verbindung verursachen. Ich habe diese bereits erläutert. Dazu gehören eine hohe Auslastung der CPU und der Netzwerkbandbreite sowie Schwierigkeiten, eine stabile Netzwerkverbindung aufrechtzuerhalten.

Auch bei einem starken Signal kann es zu Verbindungsproblemen kommen, die schwer zu entdecken sind, wenn man nicht damit rechnet. Da wären beispielsweise überlastete Netzwerke, die häufig bei großen öffentlichen Menschenansammlungen auftreten, beispielsweise bei Sportveranstaltungen, oder wenn es weitreichende Notfälle gibt (Stürme oder Überschwemmungen), die für einen rapiden Anstieg

der Netzwerknutzung sorgen. Ihr Gerät zeigt dann zwar eine fast perfekte Signalstärke an, kann aber weder Anrufe tätigen noch Textnachrichten versenden oder Daten überragen. Eine weitere Erklärung für Verbindungsprobleme trotz großer Signalstärke sind vom Mobilfunkanbieter auferlegte Einschränkungen. Beispielsweise könnte Sie beim Roaming nur niedrige Datenübertragungsraten erreichen, weil der Mobilfunkanbieter die Datenrate für Fremdkunden begrenzt. Das Überschreiten des vertraglich vereinbarten Datenkontingents kann ebenfalls zu einer Drosselung der Geschwindigkeit führen.

Üblicherweise wird der Benutzer per E-Mail oder Textnachricht davon in Kenntnis gesetzt, wenn das Datenkontingent überschritten wurde, aber manchmal übersehen die Benutzer diese Benachrichtigung. Welche Bandbreite dem Benutzer nach dem Überschreiten des Datenkontingents zur Verfügung gestellt wird, hängt vom Mobilfunkanbieter und den Vereinbarungen im Mobilfunkvertrag ab. Manche Anbieter unterbinden die Datenübertragung, andere verlangen beträchtlich höhere Gebühren oder drosseln die Datenübertragungsrate. Kompliziert ist es immer, aber die Optionen sind immer dieselben: Bezahlen Sie für ein größeres Datenkontingent oder behalten Sie das schon verbrauchte Datenkontingent im Auge und deaktivieren Sie bei Bedarf die Nutzung mobiler Daten (Abbildung 25.5).

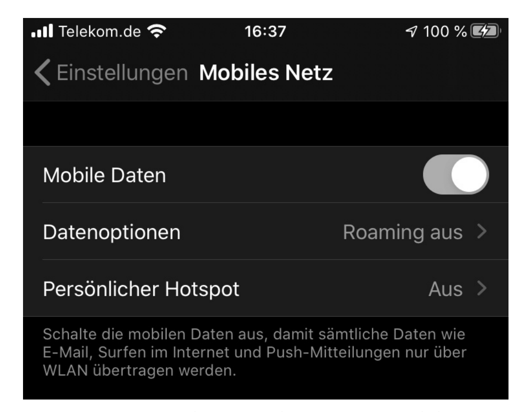


Abb. 25.5: Option zum Deaktivieren der Nutzung mobiler Daten in iOS

Bei Datenkontingenten ist vor allem wichtig, welche Folgen sie in der Praxis haben können. Wenn Ihr Unternehmen einen Mobilfunkvertrag mit Datenkontingent abgeschlossen hat, ist es äußerst hilfreich, zu wissen, was geschieht, wenn das Datenkontingent eines Benutzers überschritten wird. Was würden Sie vermuten, wenn ein Benutzer am Monatsende mit einem Gerät bei Ihnen erscheint, das plötzlich im Mobilfunknetz nur noch miserable Verbindungen per Skype ermöglicht, im WLAN aber tadellos funktioniert? Oder wenn eine Außendienstmitarbeiterin Ihnen erzählt, dass sie laufend von Kollegen angerufen wird, die wissen wollen, weshalb sie sich bei einer wichtigen Diskussion, die per E-Mail stattgefunden hat, nicht zu Wort gemeldet hat, die ihr jedoch nicht angezeigt wurde, obwohl sie stets über eine gute Verbindung verfügte? Eine kurze Überprüfung, ob das Datenkontingent überschritten wurde, kann Ihnen eine stundenlange Fehlersuche ersparen.

25.1.12 GPS und Ortungsdienste funktionieren nicht

Die Qualität der Ortungsdienste kann stark schwanken. Ein Teil der Ungenauigkeiten lässt sich durch die in dem Gerät verfügbare Hardware erklären. Ein Tablet ohne GPS, das nur mit WLAN ausgestattet ist, kann nur eine näherungsweise Position ermitteln.

Die Symptome bei Problemen mit Ortungsdiensten hängen davon ab, welche Apps sie zu nutzen versuchen. Fotos wird möglicherweise eine falsche Ortsangabe zugewiesen oder das Café, das Sie sich ausgesucht haben, weil es ganz in der Nähe liegt, ist doch weiter entfernt, als Ihr Gerät angezeigt hat. Eine Navigations-App könnte sogar überhaupt nicht in der Lage sein, Ihren Standort zu ermitteln, oder einen Standort anzeigen, von dem Sie kilometerweit entfernt sind. Weitere Symptome sind Mel-

dungen des Betriebssystems oder Anfragen von Apps, die auf Ortungsdienste angewiesen sind (Abbildung 25.6).

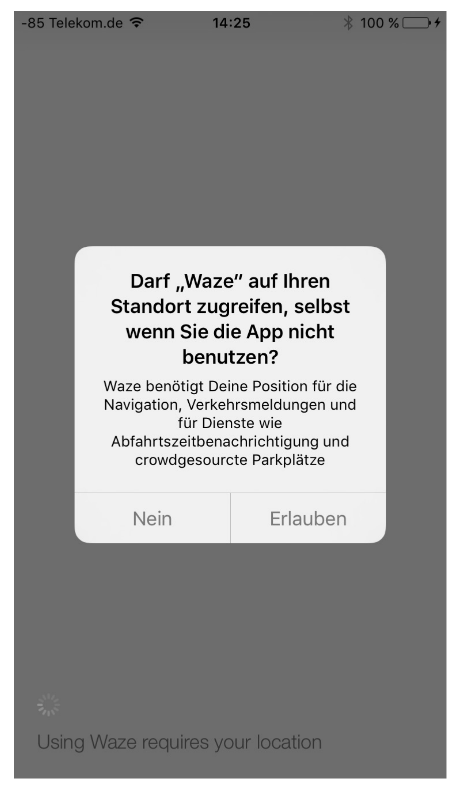


Abb. 25.6: Anforderung von Ortungsdiensten

Bei der Fehlersuche sollten Sie zuerst die naheliegenden Dinge überprüfen und sich vergewissern, dass Ortungsdienste, Mobilfunk und WLAN aktiviert sind und ordnungsgemäß arbeiten, denn gelegentlich kann es vorkommen, dass der Benutzer einen Dienst unbeabsichtigt deaktiviert oder eine App ihn abschaltet. Sie müssen den betreffenden Dienst dann nur wieder aktivieren. Normalerweise zeigen Apps eine Warnmeldung an, wenn GPS oder Datendienste nicht verfügbar sind, daher sind Probleme dieser Art leicht zu finden und zu beheben. Möglicherweise sind auch nur einzelne Apps von Problemen betroffen, wenn diese so konfiguriert worden sind, dass ihnen der Zugriff auf die Ortungsdienste untersagt ist. In diesem Fall muss entweder in der App selbst oder in den Systemeinstellungen für die Ortungsdienste der Zugriff wieder freigeschaltet werden.

Wichtig

Wenn GPS abgeschaltet ist, wird jede App, die Ortungsdienste benötigt, darauf hinweisen und Sie für gewöhnlich dazu auffordern, die Dienste zu aktivieren. Bevor Sie sich auf die Fehlersuche begeben, sollten Sie sich außerdem vergewissern, dass Sie sich an einem Ort befinden, an dem Sie ein GPS-Signal empfangen können.

Nachdem Sie die offensichtlichen Gründe für Probleme mit den Ortungsdiensten überprüft haben, die durch Software verursacht werden, sollten Sie sich die Umgebung ansehen, bevor Sie sich die vergebliche Mühe einer Fehlersuche machen. In der U-Bahn funktioniert GPS nicht, und auch im Inneren

von Häusern nur schlecht, wenn man sich nicht in der Nähe eines Fensters befindet. In dicht bebauten Stadtgebieten mit hohen Gebäuden gibt es ebenfalls Probleme. Sie brauchen also keine langwierige Fehlersuche in Angriff zu nehmen, wenn Ihr Gerät gelegentlich nicht erkennt, auf welcher Straße in der Innenstadt Sie gerade flanieren.

Wenn Sie sich sicher sind, dass sich gehäuft auftretende Probleme mit den Ortungsdiensten nicht durch die Umgebung erklären lassen, müssen Sie einen Schritt weiter gehen. Neben den vorhin erwähnten Problemen mit dem Betriebssystem könnte es systemweite Einstellungen für GPS, Mobilfunk und WLAN geben, die das ordnungsgemäße Funktionieren der Ortungsdienste verhindern. Diese Konfiguration sollte überprüft werden, wenn Symptome für Probleme mit den Ortungsdiensten bei mehr als einer App auftreten.

Wenn die Probleme weiterhin bestehen, wäre es möglich, dass die GPS- oder Netzwerk-Hardware defekt ist oder dass der Code des Betriebssystems, der darauf zugreift, fehlerhaft ist. Recherchieren Sie online, ob andere Benutzer des Geräts mit der gleichen Softwareversion von ähnlichen Problemen berichten. Ist das nicht der Fall, muss das Gerät vermutlich in die Reparaturwerkstatt. Manche Laptops und andere mobile Geräte besitzen zwar entnehmbare Funk- oder GPS-Module, diese Komponenten sind jedoch meistens nicht vom Endkunden austauschbar und müssen von autorisierten Servicetechnikern ersetzt oder repariert werden.

25.1.13 Ausgesperrt

Eine *Benutzersperre* erfolgt, wenn zu viele aufeinanderfolgende Anmeldeversuche fehlschlagen. Dadurch soll das System vor Brute-Force-Angriffen geschützt werden. Manche Anmeldemethoden, wie das Zeichnen eines einfachen Musters, bieten zwar hinreichende Sicherheit, um zu verhindern, dass jemand ein Gerät entsperrt, wenn es einen Augenblick lang unbeaufsichtigt ist. Dass jemand bei einem gestohlenen oder gefundenen Gerät alle möglichen Kombinationen ausprobiert, bis eine funktioniert, wird dadurch jedoch nicht unterbunden, zumal auf dem Bildschirm erkennbare Spuren von Fingerbewegungen die Anzahl der möglichen Kombinationen begrenzt.

Andere Sperrmechanismen blockieren für einen längeren Zeitraum Anmeldeversuche, verlangen eine Anmeldung mit vollständigen Zugangsdaten oder löschen als Vorsichtsmaßnahme alle auf dem Gerät gespeicherten Daten, wenn eine bestimmte Anzahl gescheiterter Anmeldeversuche überschritten wird. Diese Einstellung kann am Gerät selbst oder zentral über die *MDM*-Software (*Mobile Device Management*) eines Unternehmens vorgenommen werden. Sie sollten den Benutzer am besten anweisen, keinesfalls die Anzahl der erlaubten Anmeldeversuche zu überschreiten und das Gerät vor Kindern oder anderen Übeltätern zu schützen, die den Mechanismus auslösen könnten.

Wenn es sich um firmeneigene Geräte handelt, solle das Unternehmen die PINs aller Geräte an einem sicheren Ort verwahren, um im Notfall darauf zugreifen zu können, und aktuelle Sicherungskopien der mobilen Geräte anfertigen. Gehört das Gerät einem einzelnen Benutzer, kann man nur hoffen, dass er selbst Sicherungskopien angefertigt hat.

Wenn das Gerät mittels zentraler MDM-Software verwaltet wird, besteht auf jeden Fall die Möglichkeit, es vom Unternehmen aus der Ferne entsperren zu lassen. Wird es nicht zentral verwaltet, muss der Benutzer sein Gerät an einen Computer anschließen und es mit einer Software des Herstellers und einem Kennwort entsperren. Gelingt auch das nicht, besteht die einzige Lösung eventuell darin, das Gerät anhand einer Sicherungskopie wiederherzustellen, falls vorhanden, oder das Gerät auf die Werkseinstellungen zurückzusetzen.

25.1.14 Verschlüsselung

Verfahren zum Schutz von E-Mails vor dem Zugriff durch andere als den Empfänger gehören im Allgemeinen nicht zu den Lernzielen der CompTIA. Von Ihnen wird jedoch erwartet, dass Sie in der Lage sind, Fehler zu beheben, wenn ein Gerät verschlüsselte E-Mails nicht entschlüsseln kann. Um dieses Problem richtig zu verstehen, müssten wir uns mit einigen Themen befassen, die zur CompTIA-Sicherheit+-Zertifizierungsprüfung gehören. Wir betrachten hier nur die Grundlagen.

Um E-Mails zu schützen, werden sie verschlüsselt, und zwar mit einem Standard wie PGP (*Pretty Good Privacy*) oder S/MIME (*Secure/Multipurpose Internet Mail Extension*). Wenn ein Benutzer eine verschlüsselte E-Mail lesen möchte, benötigt er eine Software zum Entschlüsseln der Nachricht. Um zu gewährleisten, dass nur Sender und Empfänger auf den Inhalt der E-Mail zugreifen können, brauchen beide einen Schlüssel, der Verschlüsselung und Entschlüsselung ermöglicht. Ein Schlüssel ist eine Zeichenfolge, die ein Computer verwendet, um Daten zu verschlüsseln oder zu entschlüsseln.

In der Praxis gibt es verschiedene Gründe dafür, dass ein Gerät eine E-Mail nicht entschlüsseln kann. Meistens liegt es daran, dass der E-Mail-Client oder eine App den Verschlüsselungsstandard nicht unterstützt, der zum Verschlüsseln der E-Mail verwendet wurde. Das Problem lässt sich durch ein Plug-in oder durch den Einsatz eines anderen E-Mail-Clients beheben. Nachdem Sie sich vergewissert haben, dass ein E-Mail-Client oder eine App den Verschlüsselungsstandard unterstützt, folgen Sie den Schritten zur Konfiguration, um ihn zu verwenden. Der E-Mail-Client benötigt zum Entschlüsseln der Nachricht natürlich auch den Schlüssel. Bei einigen Standards müssen Schlüssel manuell ausgetauscht werden. Der Absender muss also kontaktiert werden, um an den Schlüssel zu gelangen. In anderen Fällen findet unter bestimmten Umständen ein automatischer Austausch der Schlüssel statt (beispielsweise wenn Sender und Empfänger derselben Organisation angehören).

25.2 Sicherheitsaspekte

Wie alle Computer, die wir zum Zugriff auf sensible Daten oder Netzwerkressourcen verwenden, müssen mobile Geräte geschützt werden. Sie müssen daher dafür sorgen, dass sowohl firmeneigene als auch private Geräte vor Beschädigung, Diebstahl und Malware geschützt sind und dass wichtige Daten nicht verloren gehen oder in die falschen Hände geraten.

25.2.1 BYOD vs. firmeneigene Geräte

Die *BYOD*-Schlacht (*Bring Your Own Device*) währte nur kurz und wurde von den Unternehmen verloren, die hofften, weiterhin die Tradition fortzuführen, dass IT-Gerätschaften nicht den einzelnen Mitarbeitern gehören, sondern der Firma (und strikt von ihr kontrolliert werden). Nachdem immer mehr mobile Geräte Teil der Infrastruktur von Unternehmen geworden waren, bemerkten schließlich auch die IT-Abteilungen, dass sich diese Entwicklung nicht mehr zurückdrehen ließ und sie niemals in der Lage sein würden, diese neuen Technologien vollständig unter Kontrolle zu bekommen. Unter bestimmten Umständen können Unternehmen Richtlinien durchsetzen, die es untersagen, private Geräte zum Zugriff auf firmeneigenen Daten und Ressourcen zu verwenden, insbesondere in Umgebungen, in denen die höchste Sicherheitsstufe gilt. Am anderen Ende des Spektrums gibt es Unternehmen, die den Einsatz privater Geräte erlauben oder sogar fördern, weil dadurch IT-Kosten gesenkt werden und die Mitarbeiter damit sehr viel zufriedener sind.

Die meisten Unternehmen und Organisation sind hier jedoch irgendwo in der Mitte einzuordnen und nutzen gemischte Umgebungen, in denen sowohl firmeneigene als auch private mobile Geräte zum Einsatz kommen. In manchen Fällen werden Kostenbeteiligungsprogramme eingerichtet und Angestellte, die ihre eigenen Geräte nutzen, erhalten zum Ausgleich einen monatlichen Zuschuss zu ihren Telefonkosten oder besondere Vergünstigungen beim Abschluss von Mobilfunkverträgen. In welchem Umfang BYOD zum Zuge kommt, spielt letztendlich keine Rolle. Es gibt hier einige Herausforderungen, die in Angriff genommen werden müssen.

Eine davon betrifft die Frage, inwieweit das Gerät unter der Kontrolle des Unternehmens oder des privaten Eigentümers steht. Wenn Firmendaten auf dem Gerät verarbeitet und gespeichert werden, sollte das Unternehmen durchaus eine gewisse Kontrolle über das Gerät ausüben können. Andererseits gehört das Gerät dem Angestellten, und er sollte ebenfalls ein Stück weit Kontrolle ausüben können. Außerdem stellt sich die Frage, wer die laufenden Kosten für die Verwendung des Geräts übernimmt. Wenn das Unternehmen dem Angestellten gestattet, bei der Arbeit sein eigenes Gerät zu verwenden, übernimmt es dann auch einen Teil der monatlichen Kosten oder entschädigt den Angestellten in irgendeiner Form?

Diese Problematik lässt sich vermutlich am besten durch formale Richtlinien und Arbeitsvorschriften lösen. Ein weiterer wichtiger Aspekt von BYOD ist die Privatsphäre des Angestellten. Wenn die Richtlinien dem Unternehmen eine gewisse Kontrolle über das Gerät einräumen, wie viel Privatsphäre bleibt dem Angestellten dann auf seinem eigenen Gerät noch? Hat das Unternehmen Einblick in private Daten oder die Möglichkeit, das Gerät des Benutzers aus der Ferne zu steuern?

Die zunehmende Verbreitung von mobilen Geräten am Arbeitsplatz hat zur Entwicklung von MDM-Richtlinien (*Mobile Device Management*) geführt. Dabei werden auf den Geräten häufig eine spezielle App und eine spezielle Infrastruktur zur Handhabung dieser Geräte eingesetzt. Diese Richtlinien legen auch die Konfigurationsoptionen für das Unternehmen und den Benutzer fest. Oder anders ausgedrückt: Sie legen fest, wer über die Konfiguration von E-Mail, Zugang zu drahtlosen Netzwerken und dergleichen entscheidet. Sie können sich sicher vorstellen, dass die MDM-Richtlinien bei großen Unternehmen eine wichtige Rolle spielen, weil sie so umfassend und komplex sind. Sie als CompTIA-A+-Techniker erleichtern beispielsweise die Installation der MDM-App oder beheben Probleme mit der erforderlichen Infrastruktur – wie beispielsweise einem überlasteten WLAN-Zugriffspunkt, weil sich alle 25 Mitarbeiter einer Abteilung gleichzeitig eine Smartwatch gekauft haben.

25.2.2 Sicherheitsanforderungen an Profile

Ein *Profil* ist eine Sammlung von Konfigurationen und Sicherheitseinstellungen, die ein Administrator zusammengestellt hat, um sie auf eine bestimmte Kategorie von Benutzern oder Geräten anzuwenden. Profile können auf unterschiedliche Weise erzeugt werden, etwa mit einer MDM-Software oder einem Programm wie Apple Configurator. Bei Profilen handelt es sich üblicherweise um Textdateien im *XML*-Format (*Extensible Markup Language*, eine erweiterbare Auszeichnungssprache), die auf den Geräten gespeichert werden, die sie benötigen. Die Entwicklung von Profilen beruht auf dem Bedarf des Unternehmens. So kann man etwa gerätespezifische Profile entwickeln, die nur für eine bestimmte Plattform, ein bestimmtes Betriebssystem oder bestimmte Geräte ausgelegt sind, sodass bei Geräten eines gewissen Typs verschiedene Dinge voreingestellt sind.

Man kann auch Profile entwickeln, die nur für bestimmte Benutzerkategorien oder Verwaltungsgruppen gültig sind (z.B. Außendienstmitarbeiter, mittleres Management oder Führungskräfte). Für die Führungskräfte könnte man ein eigenes Profil erstellen, das ihnen zusätzliche Berechtigungen und Zugriff auf spezielle Apps gewährt.

Es könnte auch gruppenspezifische Profile geben, die nur für externe Benutzer gelten, z.B. für Berater oder Geschäftsfreunde. Ein solches Profil könnte eine bestimmte Netzwerkkonfiguration oder VPN- und Sicherheitseinstellungen umfassen, damit die Gruppenmitglieder auf ein Extranet für Besucher zugreifen können. Vielleicht benötigen sie auch Zugang zu einer bestimmten B2B-App, die auf den Unternehmensservern gehostet wird. Jedenfalls können sowohl gerätespezifische als auch benutzerspezifische Profile bei der Verwaltung größerer Anwendergruppen ungemein hilfreich sein, denn sie ermöglichen einheitliche Sicherheitseinstellungen und Konfigurationen der Geräte, die sich für verschiedene Aufgaben oder geschäftliche Anforderungen anpassen lassen.

Bei Bedarf wäre es auch vorstellbar, mehrere Profile gleichzeitig auf ein Gerät anzuwenden, eines für die Plattform, eines für die Benutzergruppe usw. Unter Umständen könnte es dabei jedoch zu Konflikten kommen, z.B. wenn eine restriktive Einstellung eines Geräteprofils im Widerspruch zu einem weniger restriktiven Gruppen- oder Benutzerprofil steht. Wenn dann beide Profile auf das Gerät angewendet werden, überschreiben sie sich womöglich gegenseitig und Sie müssen auf die Rangfolge der Profile achten. Diese Rangfolge können Sie mit der MDM-Software festlegen und die Konflikte anhand verschiedener Kriterien auflösen, wie z.B. Gruppenmitgliedschaft oder Sicherheitsanforderungen.

Was die Geräte betrifft, sollten Sie neben den herstellerspezifischen und betriebssystemspezifischen Profilen auch Profile für firmeneigene und private Geräte erstellen. Die Profile für private und firmeneigene Geräte können sich erheblich voneinander unterscheiden. Das betrifft insbesondere die Richtlinien für Privatsphäre, akzeptable Nutzungsweise des Geräts usw. Abbildung 25.7 zeigt, wie Sie im Prinzip verschiedene Profile auf unterschiedliche Geräte und Benutzergruppen anwenden können.

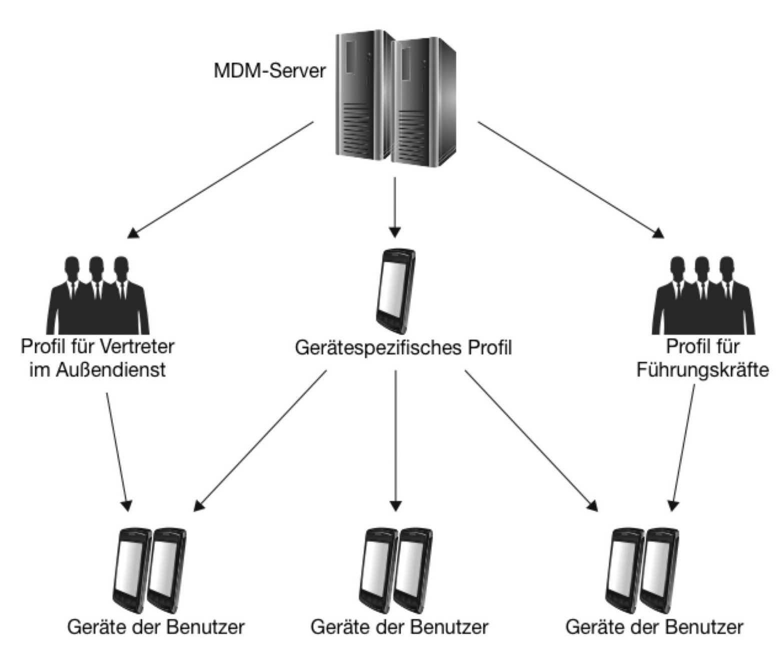


Abb. 25.7: Anwendung von Profilen auf verschiedene Geräte und Benutzergruppen

25.2.3 Beschädigung vermeiden

Die mobilen Geräte kosten eine Menge Geld und sind selbstverständlich keine Wegwerfartikel. Zum Schutz vor physischer Beschädigung sollten Sie mindestens eine Schutzhülle oder ein Etui für das mobile Gerät beschaffen. Wenn die Linse verkratzt, ist das dem Camcorder Ihres neuen iPads nicht gerade zuträglich! Die Aufnahmen sind dann verschwommen und unscharf, obwohl der Camcorder es eigentlich sehr viel besser kann. Apple bietet sehr brauchbare Schutzhüllen für iPhone und iPad an und es gibt eine Menge Hüllen und Etuis von Drittherstellern (Abbildung 25.8).



Abb. 25.8: Apple Smart Cover für ein iPad

Je nachdem, wie viel Geld Sie ausgeben möchten, stehen Ihnen Hüllen zur Verfügung, die vor Kratzern, Stößen und geringen Flüssigkeitsmengen schützen. Sie wollen mit Ihrem Android-Tablet tau-

chen? Es gibt wasserdichte Gehäuse, die es Ihnen erlauben, in zwölf Meter Wassertiefe Ihr Facebook-Konto zu aktualisieren.

Achten Sie zum Schutz Ihrer Geräte auch auf Naheliegendes. Halten Sie die Geräte von Flüssigkeiten fern. Überprüfen Sie Hemd- und Hosentaschen, bevor Sie Kleidungsstücke in die Wäsche geben, ob sich vielleicht noch ein Smartphone darin befindet. Denken Sie gar nicht erst daran, schwere Gegenstände auf einem 500-Euro-Tablet abzulegen. Hören Sie einfach auf Ihren gesunden Menschenverstand.

25.2.4 Schutz vor Malware

Malware für mobile Geräte ist ein interessantes Thema. Die strikte Kontrolle des Betriebssystems und die strenge Überprüfung von Apps macht herkömmliche Infektionen mit Malware auf iOS- und Windows-Phone-Geräten fast unmöglich. Die Betriebssystemhersteller veröffentlichen regelmäßig Patches und automatische Aktualisierungen und können so darauf reagieren, wenn tatsächlich Malware auftaucht, Bei Android fehlen einige der von iOS und Windows Phone bekannten Schutzmaßnahmen. Um diese Lücke zu schließen, bieten Dritthersteller Antiviren- und Anti-Malware-Programme für einzelne Geräte oder Unternehmensumgebungen an. In Abbildung 25.9 sehen Sie ein Beispiel einer Antiviren-Software für ein Android-Gerät.

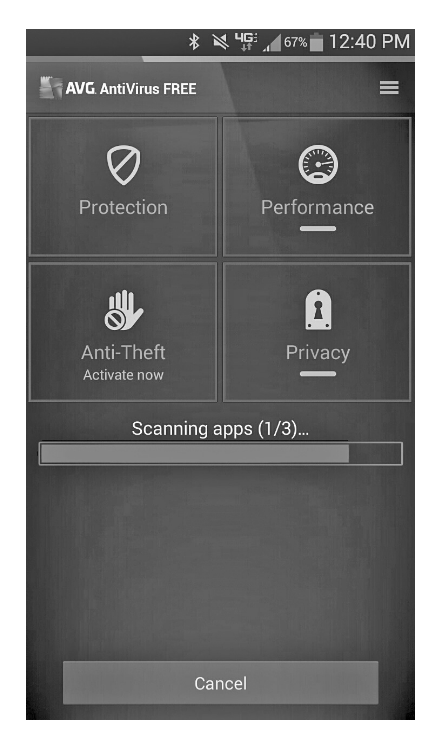


Abb. 25.9: Antivirus-App für Android

Anti-Malware-Lösungen für mobile Geräte versuchen, umfangreichen Schutz vor allen möglichen Bedrohungen zu bieten, und sollten am besten auf allen mobilen Geräten in Unternehmensumgebungen installiert sein. Da es in heterogenen Infrastrukturen eine Vielzahl unterschiedlicher Geräte von diversen Herstellern gibt, die verschiedene Betriebssysteme nutzen, wird eine einzige Anti-Malware-Lösung vermutlich nicht funktionieren. Aus diesem Grund dürften verschiedene Lösungen für die unterschiedlichen mit dem Unternehmensnetzwerk verbundenen Geräte erforderlich sein. In einigen Fällen stellen die Hersteller auch verschiedene Module für unterschiedliche Gerätetypen zur Verfügung, um die Rechner in Unternehmensumgebungen zu schützen.

Auf jeden Fall ist es wichtig, dass bei einer Anti-Malware-Lösung in Unternehmensumgebungen regelmäßig eine Aktualisierung der Geräte durchgeführt wird. Lösungen zur Zugriffssteuerung auf das Netzwerk können gewährleisten, dass bei allen Geräten, die sich mit dem Netzwerk verbinden wollen, überprüft wird, ob die neuesten Malware- und Virensignaturen vorhanden sind und diese bei Bedarf aktualisieren, bevor die Verbindung zugelassen wird. Falls vom Benutzer einzurichtende Anti-Malware-Programme eingesetzt werden, sollte es Richtlinien, Zugriffskontrollen und andere technische Lösungen geben, die sicherstellen, dass die Anwender ihre Geräte regelmäßig aktualisieren.

25.2.5 Maßnahmen bei Verlust

Am besten bereiten Sie sich auf den Verlust eines Smartphones oder Tablets vor, indem Sie davon ausgehen, dass es zwangsläufig passieren wird. Alle mobilen Geräte gehen irgendwann einmal verloren. Ich kann nur hoffen, dass die meisten Ihrer Anwender diese Behauptung widerlegen, aber die Chancen stehen nicht schlecht, dass wir alle unsere Geräte mindestens einmal verlieren. Meistens hat man Glück und findet das Gerät dort, wo man es liegen gelassen hat, aber es kann auch anders kommen.

Für den Fall des Verlusts eines Smartphones oder Tablets ist eine ganze Menge zu bedenken. Zunächst sollten Sie Ihre Daten durch ein vernünftiges Kennwort oder eine andere Sperre (z.B. eine Verriegelung, die durch das Zeichnen eines bestimmten Musters aufgehoben wird, einen Fingerabdruckscanner oder sogar durch Gesichtserkennung) schützen (Abbildung 25.10).

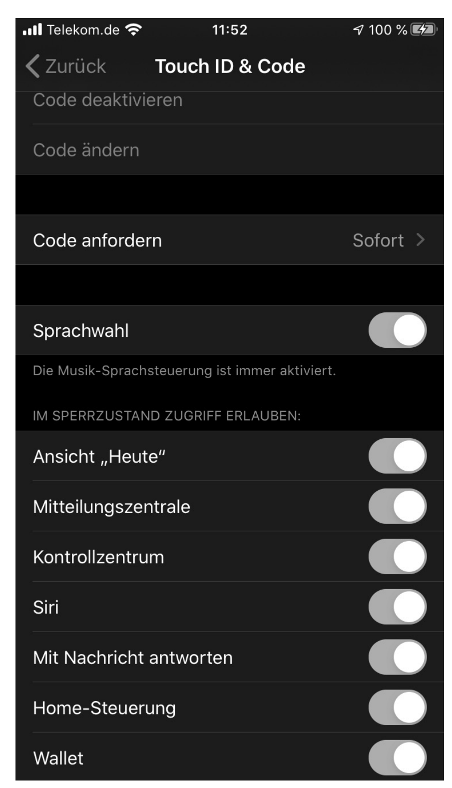


Abb. 25.10: Code-Sperre in der App EINSTELLUNGEN

Zögern Sie nicht länger und richten Sie den Schutz jetzt ein! Bei aktuellen iOS- und Android-Geräten können Sie sämtliche Speicherinhalte verschlüsseln. Der mögliche »Finder« gelangt dann selbst nach dem Zerlegen des Geräts und Ausbau des Laufwerks nicht an Ihre Dokumente.

Hinweis

In Kapitel 27, *Computersicherheit*, gehe ich sehr viel ausführlicher auf Malware und verschiedene Typen von Schadsoftware sowie deren Herkunft und die Symptome einer Infektion ein.

Wichtig

Zum Entsperren des Smartphones oder Tablets gibt es verschiedene Methoden, beispielsweise Fingerabdruckscanner, Zeichnen eines Musters, Gesichtserkennung oder Eingabe eines Entsperrcodes.

Es ist außerdem möglich, beim Überschreiten einer voreinstellbaren Zahl von Fehlversuchen bei der Anmeldung weitere Restriktionen in Kraft zu setzen, beispielsweise die Anmeldung für einen längeren Zeitraum zu sperren. Dadurch gewinnen Sie Zeit, wenn jemand versucht, sich in ein gefundenes Gerät einzuhacken, und Sie dabei sind, es durch die Ortungsdienste wieder aufzufinden oder aus der Ferne zu löschen.

Wichtig

Bei vielen Geräten ist es möglich, nach einer bestimmten Anzahl gescheiterter Anmeldeversuche zusätzliche Restriktionen in Kraft zu setzen oder sogar automatisch alle Inhalte des Geräts zu löschen.

Apple und Google bieten Dienste an, mit denen sich verloren gegangene Geräte wiederfinden lassen. Melden Sie sich z.B. bei Ihrem iCloud-Konto an und klicken Sie auf die Schaltfläche IPHONE-SUCHE. (Das funktioniert auch mit iPad und iPod touch.) Sobald das Gerät mit dem Internet verbunden wird (und eine IP-Adresse erhält und seine MAC-Adresse meldet), lokalisiert iCloud das Gerät auf wenige Meter genau und zeigt die Position auf einer Landkarte an (Abbildung 25.11). Sehr clever!

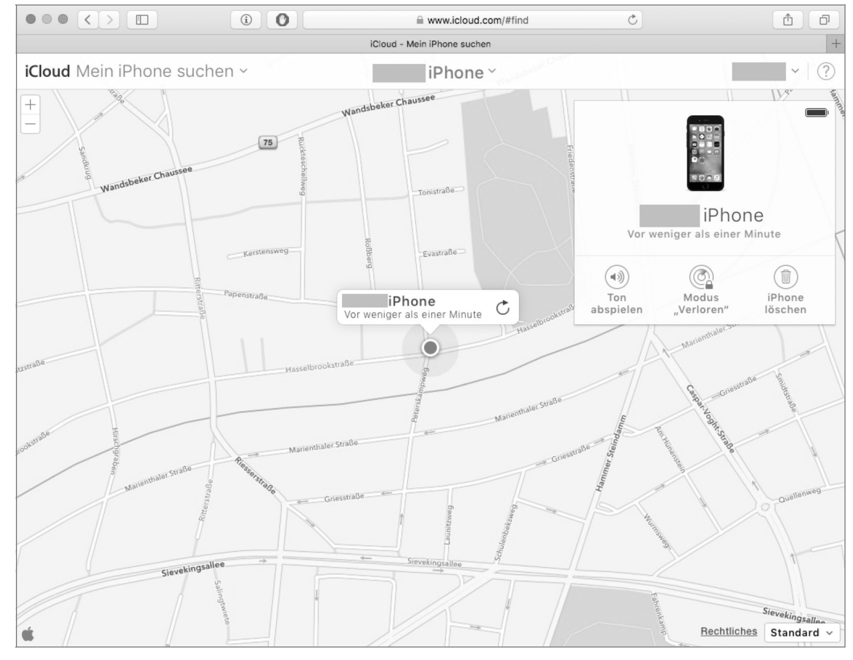


Abb. 25.11: iPhone-Suche

25.2.6 Diebstahl

Falls Ihr Gerät gestohlen wird und sich schützenswerte Daten darauf befinden, stehen Ihnen verschiedene Möglichkeiten offen. Die Ortungsdienste sind sicherlich hilfreich, aber wenn sich beispielsweise Kreditkartendaten oder andere potenziell schädigende Informationen auf dem Gerät befinden, müssen Sie schnell handeln.

Stellen Sie zuerst sicher, dass Sie eine Sicherungskopie der Daten besitzen. Im Normalfall sollte alles mit dem lokalen Rechner synchronisiert sein und, falls möglich, eine Sicherungskopie auf einem Dienst wie Microsofts OneDrive hinterlegt sein, sodass Ihre Daten selbst beim Verschwinden Ihres Hauses noch verfügbar sind. Wenn Sie Windows Phone verwenden, rufen Sie in den Einstellungen das Backup auf. Auf diesem Bildschirm können Sie auswählen, welche Daten gesichert werden (Abbildung 25.12).

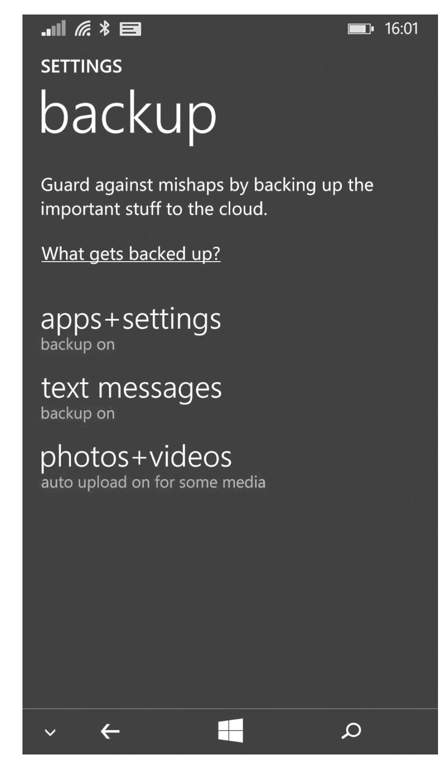


Abb. 25.12: Auswahl der zu sichernden Daten

Die Inhalte von Apple-Geräte können Sie mit einem der Dienste iTunes oder iCloud sichern und mit dem Apple Configurator wiederherstellen. Android-Geräte nutzen zum Sichern und Wiederherstellen Google Sync.

Eine weitere Möglichkeit ist das Löschen aller Daten auf dem mobilen Gerät aus der Ferne (*Remote Wipe*). Apple beispielsweise macht es Ihnen wirklich äußerst leicht: Melden Sie sich an, lokalisieren Sie das Gerät und machen Sie es platt (Abbildung 25.13)! Sie sehen es womöglich nie wieder, aber immerhin haben die Halunken keinen Zugriff auf Ihre Daten. Bei Android-Geräten ist es genauso einfach. Melden Sie sich an, lokalisieren Sie Ihr Gerät und löschen Sie die Daten.



Abb. 25.13: Remote Wipe eines iPhones

25.2.7 Daten schützen

Mit Ausnahme des Remote Wipes ging es bisher immer darum, das Gerät selbst zu schützen. Sehen wir uns nun an, was man zum Schutz der eigentlichen Daten unternehmen kann.

Mehrfaktor-Authentifizierung

Die Begriffe *Mehrfaktor-Authentifizierung* und *Ein-Faktor-Authentifizierung* machen den Unterschied schon klar: die Anzahl der zur Authentifizierung erforderlichen Faktoren. Unklar bleibt, was ein Authentifizierungsfaktor eigentlich ist und weshalb eines der verbreitetsten Authentifizierungsverfahren – Benutzername und Kennwort – eine Ein-Faktor-Authentifizierung ist. Sehen wir uns die drei wichtigsten Faktoren an. Der erste Faktor ist Wissen. Wissen bedeutet, dass dem Benutzer bestimmte Informationen bekannt sein müssen, etwa ein Benutzername und das zugehörige Kennwort, ein Geburtsdatum, die Sozialversicherungsnummer etc. Der zweite Faktor ist Besitz. Mit Besitz ist gemeint, dass der Benutzer über einen bestimmten Gegenstand verfügen muss, beispielsweise eine Ausweiskarte oder einen Identifizierungschip. Beim dritten Faktor, der Biometrie, dient der Benutzer selbst zur Authentifizierung, wobei z.B. Fingerabdrücke oder Netzhautmuster überprüft werden. Diese drei Faktoren werden oft beschrieben als etwas, das der Benutzer *weiß*, *hat* und *ist*.

Es gibt noch andere Authentifizierungsfaktoren, die allerdings beim Schutz von Daten keine große Rolle spielen. Ein weiterer Authentifizierungsfaktor ist beispielsweise der Aufenthaltsort. Er kann verwendet werden, wenn sich die Position einer Person per GPS oder auf andere Weise ermitteln lässt. So könnte es beispielsweise erforderlich sein, dass sich eine Person an einem bestimmten Ort aufhalten muss, um sich bei einem System anmelden zu können. Auch die Zeit kann ein Authentifizierungsfaktor sein. Die Anmeldung könnte etwa nur zu einer bestimmten Tageszeit erlaubt sein, nur innerhalb eines kurzen Zeitraums, oder nur ein paar Sekunden oder Minuten lang, nachdem ein anderer Vorgang stattgefunden hat. Chipkarten, die einen Code anzeigen, nutzen ebenfalls die Zeit als Authentifizierungsfaktor, denn die angezeigten Codes sind nur für kurze Zeit gültig.

Nun sind Ihnen Authentifizierungsfaktoren bekannt und wir können wieder auf die einfachste Form zurückkommen, die Ein-Faktor-Authentifizierung. Der Benutzer muss in diesem Fall nur einen der Faktoren zur Authentifizierung einsetzen. Am häufigsten begegnet man dieser Authentifizierungsmethode in Form einer Kombination aus Benutzername und Kennwort. Beides sind Dinge, die man weiß, deshalb kommt hier nur ein Faktor zum Tragen, das Wissen. Ein klassisches Türschloss ist ebenfalls ein Ein-Faktor-Authentifizierungsverfahren, denn der erforderliche Schlüssel stellt einen Faktor dar, nämlich Besitz.

Früher war die Bezeichnung Zwei-Faktor-Authentifizierung geläufiger, die logischerweise zwei Faktoren nutzt. Im Laufe der Jahre wurden allerdings Authentifizierungsverfahren entwickelt, die sogar mehr als zwei Faktoren verwenden, daher ist es besser, jetzt die Bezeichnung Mehrfaktor-Authentifizierung zu gebrauchen. Bei einer Mehrfaktor-Authentifizierung kann eine Vielzahl von Verfahren zum Einsatz kommen – sofern sie denn mehr als einen Faktor einsetzen.

Nur weil der Begriff schick ist und uns an komplexe Systeme in geheimen Institutionen der Regierung denken lässt, dürfen Sie nicht glauben, dass die Mehrfaktor-Authentifizierung nicht schon seit Jahrzehnten im Alltag eine wichtige Rolle spielt. Wenn Sie sich z.B. an einem Geldautomaten Bargeld holen, verwenden Sie eine Mehrfaktor-Authentifizierung: Sie benutzen die Bankkarte (Faktor Besitz) und Ihre PIN (Faktor Wissen), um an Ihr Geld zu gelangen.

Wichtig

Verwechseln Sie die Kombination aus Benutzername und Kennwort nicht mit einer Mehrfaktor-Authentifizierung. Zur Anmeldung sind zwar zwei Dinge erforderlich, die aber beide zur Kategorie »Wissen« gehören. Die Kombination aus Benutzername und Kennwort ist daher eine Form der Ein-Faktor-Authentifizierung.

Biometrische Authentifizierung

Kombiniert mit anderen Authentifizierungsfaktoren stellen biometrische Geräte ein sehr sicheres Authentifizierungsverfahren dar. Ein Beispiel hierfür: Sie präsentieren Ihre persönliche Smartcard einem Kartenleser und legen dann Ihren Finger auf einen Fingerabdruckscanner. Daraufhin erhalten Sie Zugang zu einer Sicherheitszone.

Mobile Geräte verwenden mittlerweile ebenfalls biometrische Geräte. Laptops sind schon seit einigen Jahren mit Fingerabdruckscannern ausgestattet, nun kommt diese Technologie auch z.B. bei Smartphones zum Einsatz. Das beste Beispiel hierfür ist Apples Touch ID. Seit dem iPhone 5S können die Apple-Geräte durch einen Fingerabdruck entsperrt werden. Um Touch ID zu aktivieren, müssen Sie in der App Einstellungen mindestens einen Fingerabdruck hinterlegen – Sie können aber auch mehrere Finger registrieren (Abbildung 25.14). Aktuelle Geräte verwenden zur Identifizierung und Authentifizierung des Benutzers Gesichtserkennung.

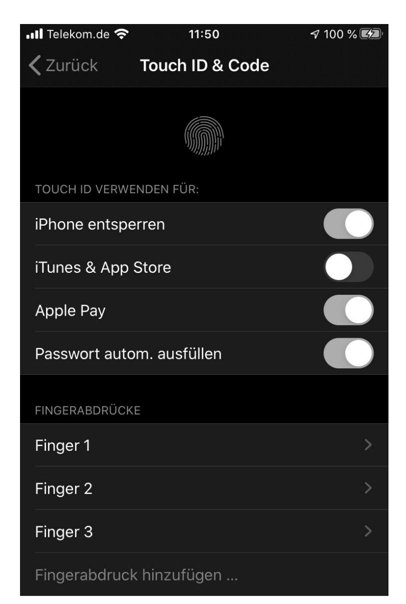


Abb. 25.14: Optionen von Touch ID

Authentifizierung in der Praxis

Für den Zugriff auf Unternehmensnetzwerke sind oft sichere Authentifizierungsmethoden erforderlich. Um beispielsweise auf den VPN-Server eines Unternehmensnetzwerks zuzugreifen, könnte eine von dem Unternehmen zu diesem Zweck freigegebene und veröffentlichte spezielle App notwendig sein, die für die korrekten Sicherheitseinstellungen sorgt. Darüber hinaus gibt es auch allgemeine Anwendungen, die verschiedene Authentifizierungsmethoden unterstützen und es ermöglichen, die Zugangsdaten zu mehreren Websites, Netzwerken oder netzbasierten Diensten (wie E-Mail, VPN-Zugang usw.) zu verwalten. Außerdem gibt es eine Reihe von Apps, die Mehrfaktor-Authentifizierung beherrschen und als Token dienen oder nur für eine Sitzung geltende PINs vergeben.

Bei allen Apps dieser Art spielt die Konfiguration die entscheidende Rolle. Sie benötigen die richtige Netzwerkkonfiguration, die richtigen Einstellungen für Authentifizierung oder Verschlüsselung oder eine ordnungsgemäße Registrierung durch eine entsprechende App.

Vertrauenswürdige und nicht vertrauenswürdige Quellen

Im Großen und Ganzen ist die Beschaffung von Software in den rechtmäßigen App-Stores der großen Anbieter wie Apple, Google, Microsoft oder Amazon nicht nur einfach, sondern für gewöhnlich auch sicher. Die verschiedenen Anbieter stellen unterschiedliche Anforderungen an die Entwickler, die ihre Anwendungen in den App-Stores anbieten möchten – und das betrifft auch die Anforderungen an die Sicherheit. Zum Teil hängen diese von dem Modell ab, das die Anbieter für die Entwicklung und den Support vorsehen.

Apple kontrolliert alle Aspekte der Geräte und der im App-Store verfügbaren Apps streng. (Unternehmen können jedoch selbst entwickelte Apps unternehmensintern verteilen.) Für die angebotenen Apps gelten äußerst strikte Vorgaben. Android hingegen wird nicht so streng kontrolliert. Das wird beispielsweise daran deutlich, dass Apps aus nicht vertrauenswürdigen Quellen installiert werden können.

Zwischen den verschiedenen Android-Varianten gibt es Abweichungen, denn die Hersteller können ändern, welche Quellen als vertrauenswürdig betrachtet werden und welche nicht. Wenn ein Programm auf dem Gerät eines Herstellers läuft, heißt das noch lange nicht, dass es auf dem Gerät eines anderen Herstellers ebenfalls funktioniert, obwohl auf beiden Varianten des Betriebssystems Android laufen. Das beste Beispiel hierfür sind Amazons Geräte der Kindle-Produktreihe, die Apps ausschließlich über Amazons App-Store beziehen können. Außerdem unterliegen Apps bei Google Play nicht denselben strengen Richtlinien für Entwickler, wie es bei Apple-Apps der Fall ist. Das bedeutet nicht notwendigerweise, dass sie weniger sicher sind, es wäre jedoch denkbar.

Die Sicherheitsschwachstellen, die es in über App Stores von Drittanbietern vertriebenen Apps gibt, handelt man sich nur ein, wenn man Apps aus nicht anerkannten oder inoffiziellen Quellen bezieht. Neben Google Play gibt es durchaus einige seriöse Quellen für Apps, beispielsweise die App-Stores der diversen Gerätehersteller, diejenigen der Mobilfunkanbieter oder Quellen für unternehmensintern entwickelte Software. Andere Quellen sind allerdings weniger seriös und werden von Geräteherstellern und Unternehmenskunden nicht akzeptiert. Es kann sogar erforderlich sein, das Betriebssystem zu modifizieren, um diesen Quellen entstammende Apps zum Laufen zu bringen. Lesen Sie hierzu auch den Abschnitt 25.3.4, *Unautorisierter Root-Zugriff*.

Apps aus fragwürdigen Quellen können Malware enthalten, persönliche Daten stehlen und an Dritte übermitteln. Außerdem gibt es Apps, die es erforderlich machen, das Betriebssystem des Geräts durch ein vom Hersteller nicht freigegebenes zu ersetzen. Dadurch geht in der Regel nicht nur die Garantie verloren, man läuft auch Gefahr, dass das Gerät nicht stabil läuft und nicht mehr ordnungsgemäß arbeitet.

Firewalls

In Kapitel 27 werde ich näher auf Firewalls eingehen. An dieser Stelle reicht es zu wissen, dass Software-Firewalls einen einzelnen Host vor Bedrohungen aus dem Netzwerk schützen sollen. Welche

Kenntnisse über Firewalls für mobile Geräte die CompTIA von Ihnen erwartet, ist ein wenig unklar. Im Allgemeinen verwenden mobile Geräte keine Firewall, weil es kaum Dienste gibt, die auf offenen Ports horchen, wie es bei normalen PCs der Fall ist. Da also auf den Ports gar nicht gehorcht wird, verfügen sie sozusagen über eine De-facto-Firewall. Das gilt für WLAN- und Mobilfunkverbindungen gleichermaßen, sodass die vernetzten Geräte geschützt sind. Je nach Betriebssystemversion können Sie auf Android-Systemen eine klassische Firewall installieren. Abbildung 25.15 zeigt ein Beispiel einer solchen Firewall für Android.

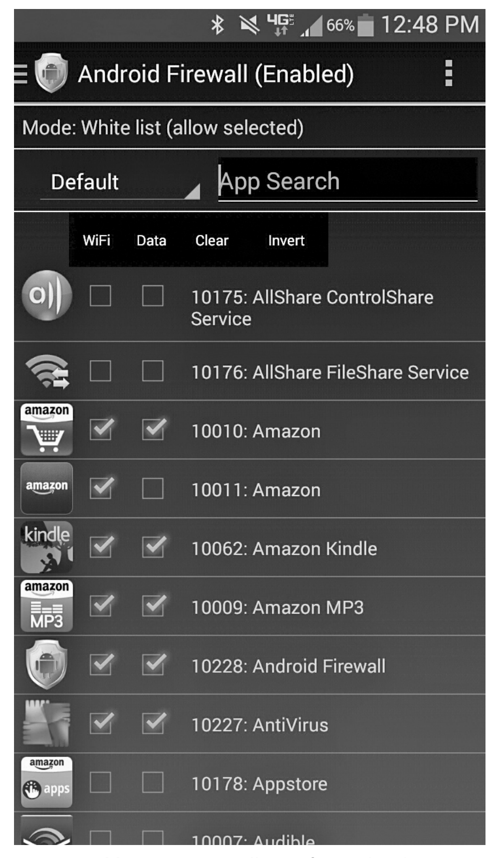


Abb. 25.15: Firewall-App für Android

Zu einer Software-Firewall gehören grundlegende Elemente, die dazu verwendet werden, Regeln zu konstruieren, die bestimmten eingehenden Datenverkehr filtern. Viele dieser Programmpakete enthalten auch Anti-Malware-Lösungen und einfache Angriffserkennungssysteme (*IDS*, *Intrusion Detection System*).

Manche dieser Software-Firewall-Lösungen sind eigenständig und müssen vom Benutzer selbst konfiguriert und verwaltet werden. Lösungen für Unternehmenskunden lassen sich hingegen an zentraler Stelle vom Systemadministrator konfigurieren, aktualisieren und verwalten. Beachten Sie hier, dass Software-Firewalls auf ganz grundlegender Ebene arbeiten und vermutlich nicht für alle möglichen Bedrohungen gewappnet sind, denen ein Host im Netzwerk ausgesetzt ist. Sie dienen jedoch als zweite Verteidigungslinie zum Schutz des Hosts und sind Bestandteil eines vernünftigen mehrstufigen Sicherheitskonzepts.

25.3 Sicherheitsprobleme auf Betriebssystem- und Anwendungsebene

Sicherheit ist ein kompliziertes Thema, das nie zur Ruhe kommt. Ich habe in diesem Kapitel schon in verschiedenen Zusammenhängen Sicherheitsaspekte erwähnt, es lohnt aber, einige weitere mögliche Sicherheitsprobleme zu betrachten. Dieser Probleme müssen sich sowohl Unternehmen als auch die einzelnen Anwender bewusst sein, und es sollten entsprechende Vorsichtsmaßnahmen getroffen werden. Wir betrachten zunächst die Werkzeuge, die Sie bei der Fehlersuche und bei Sicherheitsproblemen einsetzen können. Anschließend sehen wir uns einige der typischen Risiken, Symptome und Hinweise an, die bei Sicherheitsproblemen in Erscheinung treten können.

25.3.1 Werkzeuge zur Fehlersuche

Es gehört zu den Grundlagen der Sicherheit, sich bezüglich möglicher Bedrohungen auf dem Laufenden zu halten und auf Patches, Konfigurationsaktualisierungen, geänderte Richtlinien und Updates für Anti-Malware zu achten. Zudem sind regelmäßige Benutzerschulungen erforderlich, um auf neue Bedrohungen aufmerksam zu machen. Diese Grundlagen dienen dazu, es Angreifern nicht allzu einfach zu machen. Darüber hinaus muss man sich um Sicherheitsprobleme kümmern, die kontinuierliche Wachsamkeit erfordern: neue Bedrohungen, Vermeidung unsicherer Anwendungen und nicht korrigierbare Schwachstellen.

Die größte Bedeutung kommt Ihrem Misstrauen, Ihrem Instinkt und Ihrer Hartnäckigkeit zu, sie sollten aber nicht auf die Vielfalt technischer Werkzeuge verzichten, die Sie bei der Behebung von Sicherheitsproblemen einsetzen können. Betrachten wir also einige dieser Werkzeuge, gruppiert nach den Problemen, für deren Lösung sie am nützlichsten sind: Angriffe über das Netzwerk und die Sicherheit von Anwendungen.

Angriffe über das Netzwerk

Mobile Geräte sind grundsätzlich für ein geselliges Miteinander ausgelegt, weil sie auf diese Weise nützlicher sind, aber bei einem Angriff über das Netzwerk lässt sich diese Offenheit ausnutzen. Im Abschnitt *Ungewollte Verbindungen* sehen wir uns einige dieser Probleme an, aber zunächst konzentrieren wir uns auf Werkzeuge zum Erkennen und Entschärfen von Risiken: Sicherheitseinstellungen, Benutzerschulung sowie WLAN- und Funkzellen-Analyzer.

Sicherheitseinstellungen Grundsätzlichen fallen am ehesten Geräte einem Angriff über das Netzwerk zum Opfer, die sich allzu bereitwillig verbinden möchten. Der erste Schritt zur Entschärfung dieser Bedrohung besteht deshalb darin, zu gewährleisten, dass sich die Geräte nicht automatisch mit jedem beliebigen WLAN oder in der Nähe befindlichen Bluetooth-Geräten verbinden. Sie können diese Einstellung bei jedem Gerät einzeln vornehmen oder eine MDM-Software verwenden, mit der sich mehrere Geräte verwalten lassen, wie z.B. Apple Configurator.

Benutzerschulung Das Ändern der Sicherheitseinstellungen wird kaum einen Nutzen haben, wenn sich die Benutzer weiterhin mit jedem offenen WLAN verbinden oder jeder Kopplung mit einem Bluetooth-Gerät zustimmen, ohne über die Konsequenzen nachzudenken. Ihr Netzwerk kann auch bedroht sein, wenn die Benutzer die Hinweise darauf ignorieren, dass sich in die Verbindung mit dem sicheren Unternehmens-WLAN ein böser Zwilling des Zugriffspunkts eingeschlichen hat. Erklären Sie ihnen, wie es sich normalerweise verhalten sollte, und weisen Sie sie an, die Verbindung sofort zu unterbrechen und Bericht zu erstatten, wenn etwas Ungewöhnliches geschieht.

WLAN-Analyzer Mit einem WLAN-Analyzer können Sie nicht nur herausfinden, welche Kanäle Sie verwenden sollten, den Standort des Zugriffspunkts optimieren und Funklöcher aufspüren, sondern auch in der Nähe befindliche WLANs kartieren (Abbildung 25.16). Normalerweise werden das echte Netzwerke in umliegenden Gebäuden oder Büros sein, aber man kann nie wissen, ob nicht doch jemand mit bösen Absichten einen Zugriffspunkt eingerichtet hat.

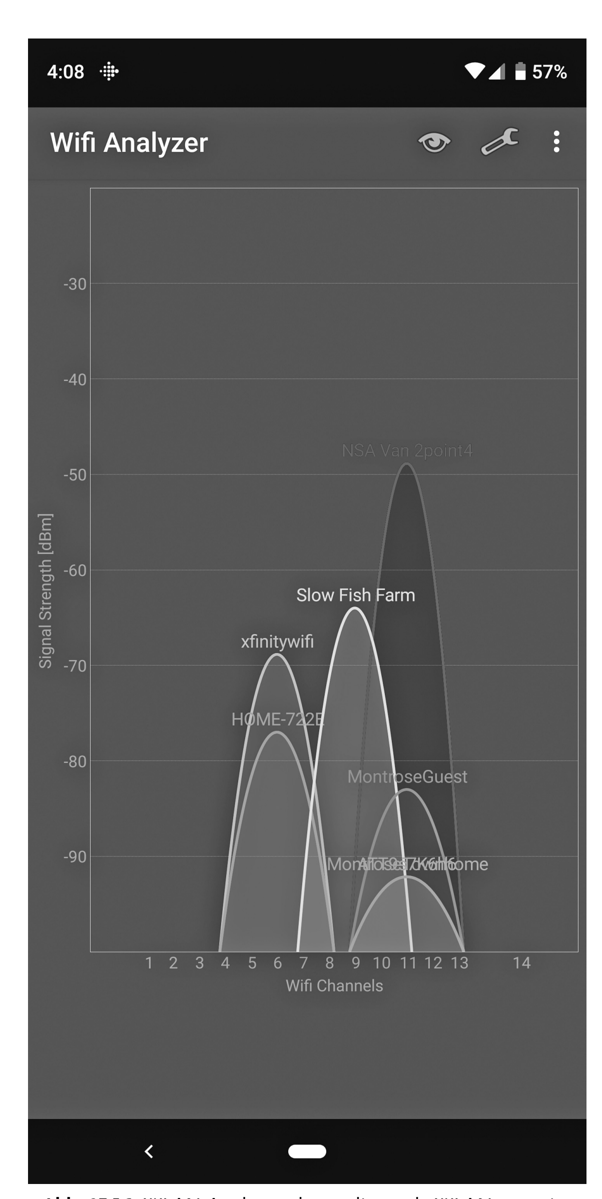


Abb. 25.16: WLAN-Analyzer, der umliegende WLANs anzeigt

Funkzellen-Analyzer Ein Funkzellen-Analyzer identifiziert – ähnlich wie ein WLAN-Analyzer – Mobilfunksignale und schätzt den Abstand zum Mobilfunksendemast, gibt die ungefähre Richtung an, in der er sich befindet, misst die Signalstärke und sammelt weitere Informationen, wie die verwendete Funktechnologie, Netzwerknamen und so weiter (Abbildung 25.17). Sie können einen Funkzellen-Analyzer beispielsweise dazu verwenden, die Signalqualität zu messen, wenn ein Benutzer Verbindungsprobleme hat, oder die Zugriffsmöglichkeiten in einem Gebäude zu kartieren. Auch hier besteht die Möglichkeit, eine unrechtmäßige Funkzelle zu entdecken – und Ihr Unternehmen könnte das Angriffsziel sein.

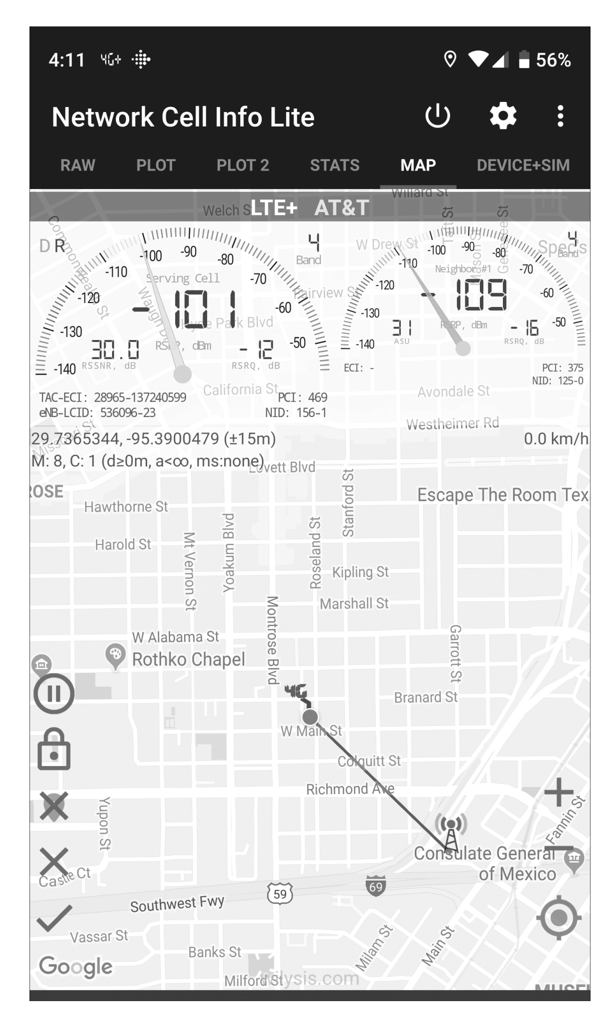


Abb. 25.17: Ein Funkzellen-Analyzer für Android schätzt die Entfernung zum Sendemast.

Sicherheit von Anwendungen

Man muss sich darüber im Klaren sein, dass die »beste« Schadsoftware ihr Ziel erreicht, ohne bemerkt zu werden. Fast jeder kann herausfinden, dass eine Schadsoftware dafür verantwortlich ist, wenn ein Gerät plötzlich extrem langsam arbeitet und sie ständig auf Webseiten umleitet, die verkünden, dass Sie eine Rundreise zum Mars gewonnen haben. Da die gefährlichste Schadsoftware zurückhaltend agiert, müssen Sie Werkzeuge verwenden, die Ihnen dabei helfen, die einfachen Varianten zu entdecken, damit Sie Ihre Aufmerksamkeit auf die subtilen Hinweise richten können, dass etwas nicht stimmt.

Anti-Malware und App-Scanner Anti-Malware-Apps für mobile Geräte verwenden – wie ihre Desktop-Pendants – Signaturen und Listen, um bekannte Schadsoftware zu identifizieren, zu blockieren, zu entfernen oder zumindest davor zu warnen. Ein *App-Scanner* hingegen durchsucht die den installierten Apps gewährten Berechtigungen, um zu beurteilen, welches Risiko sie für Sicherheit und Privatsphäre darstellen. Es gibt Apps, die nur eine der genannten Aufgaben erledigen, aber auch solche, die in der Lage sind, beide zu übernehmen. Für iOS gibt es derartige Apps nicht, aber viele der Features sind über die Einstellungen verfügbar.

App-Scanner werden typischerweise vor der Installation oder Aktualisierung einer App ausgeführt und können Sie darüber informieren, welche Netzwerkverbindung und welche Berechtigungen eine App benötigt und auf welche Hardware und Funktionen des Geräts sie zugreifen möchte.

App-Scanner können Ihnen auch anzeigen, welche Art von Zugriff eine App auf Ihre persönlichen Daten hat, wie beispielsweise Kontakte oder Mediendateien (Abbildung 25.18).

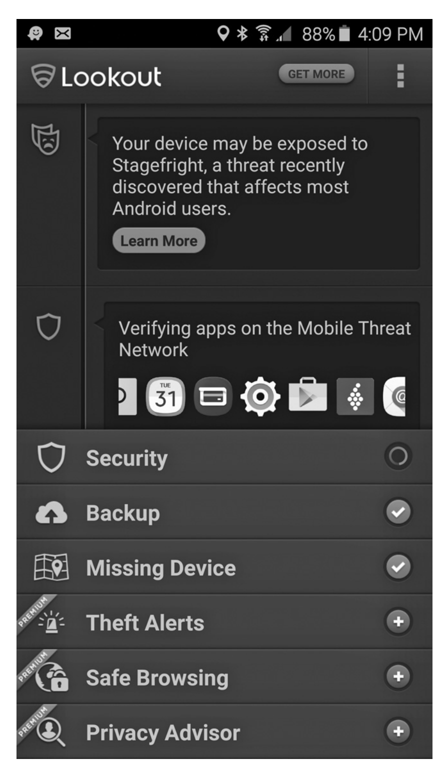


Abb. 25.18: Kombination aus Anti-Malware und App-Scanner

Sichern und Wiederherstellen Das Erstellen von aktuellen Backups ist unverzichtbar, denn sie sind der letzte Ausweg, wenn alles andere nicht funktioniert. Zu den Werkzeugen, mit denen man Backups erstellen kann, gehören MDM-Software, iTunes und die verschiedenen Synchronisierungsprogramme für Android und Windows Phone. Eine weitere Option ist das Sichern der Daten auf dem Cloud-Speicher des Herstellers, wie Microsoft OneDrive oder Apple iCloud.

Manche Schadsoftware kann sich tief im System verwurzeln, und es kann schwierig sein, sie zu entfernen. Wenn Sie ein vollständiges Backup einspielen, das zu einem Zeitpunkt vor der Infektion erstellt wurde, können Sie sich sicher sein, dass Sie die Schadsoftware los sind, und Sie müssen sich nicht ständig vergewissern, dass keine wichtigen Daten verloren gehen.

Werkzeuge zur Fehlerbehebung bei Apps Wir haben uns bereits verschiedene Werkzeuge zur allgemeinen Fehlerbehebung angesehen: das sofortige Beenden, Deinstallation und Neuinstallation einer App oder das Zurücksetzen auf die Werkseinstellungen. Sie können diese Werkzeuge auch dazu einsetzen, Sicherheitsprobleme bei Apps zu ermitteln und in Angriff zu nehmen.

Sobald Sie Symptome einer Schadsoftware oder Hinweise auf ein anderes Sicherheitsproblem bemerken, können Sie die laufenden Apps der Reihe nach beenden, bis Sie die Ursache des Problems gefunden haben. Wenn Sie wissen, welche App das Problem verursacht, sollten Sie die App deinstallieren. Wenn es sich um eine seriöse App handelt und die Symptome harmlos sind, können Sie die App

erneut installieren und prüfen, ob das Problem dadurch behoben wurde. Wenn sich das Verhalten nicht ändert, sollten Sie das Gerät auf die Werkseinstellungen zurücksetzen.

25.3.2 Risiken, Symptome und Hinweise

Von welchem Wert Misstrauen, Intuition und Hartnäckigkeit sind, wird deutlich, wenn wir die Risiken, Symptome und Hinweise betrachten, für die das Vorhandensein von Schadsoftware oder eines anderen Sicherheitsproblems verantwortlich ist.

Wenn Sie hier von einem potenziellen Risiko lesen, sollten Sie nicht davon ausgehen, dass es vereinzelt auftritt. Da Schadsoftware und andere Angriffe durchaus kreativ, komplex und facettenreich sein können, sollten Sie die nachfolgend beschriebenen Szenarien als Risiko betrachten, das es zu verstehen und zu handhaben gilt, als Symptome für Schadsoftware oder einen Angriff oder zumindest als Hinweise auf einen bevorstehenden Angriff.

Ebenso wenig, wie Sie annehmen sollten, dass die genannten Dinge als einzelne Vorkommnisse auftreten, sollten Sie auch nicht davon ausgehen, dass notwendigerweise Schadsoftware vorhanden oder ein Angriff im Gange ist, wenn Sie einem oder mehreren davon begegnen. Tatsächlich habe ich viele der genannten Probleme bereits erläutert, weil sie oft im Zusammenhang mit anderen Problemen bei mobilen Geräten auftreten.

Unerwartete Ressourcennutzung

Im Grunde genommen ist Malware nichts weiter als Software, die Ihr Gerät ohne Ihr Einverständnis für bestimmte Aufgaben nutzt. Wie jedes Programm, das Schwerstarbeit verrichtet, kann Malware Probleme bei der Verfügbarkeit von Ressourcen verursachen. Da solche Probleme auch relativ harmlos sein können und sich durch einen Warmstart beheben lassen, werden sie oft achselzuckend hingenommen. Seien Sie misstrauisch, insbesondere wenn ein Muster erkennbar ist und es keine offensichtliche Erklärung für die Probleme gibt. Eine plötzliche Zunahme der ausgehenden Daten von befallenen Mobilfunkgeräten könnte sehr wohl der erste Hinweis darauf sein, dass jemand versucht, Ihr Unternehmen auszuspionieren.

Zunahme des Energieverbrauchs und hohe Ressourcennutzung Ein heißes Smartphone, hohe Ressourcennutzung und Zunahme des Energieverbrauchs sind üblicherweise Anzeichen, dass eine App abgestürzt ist oder nicht richtig funktioniert, können aber auch Symptome dafür sein, dass Ihr Gerät genau das tut, was der Entwickler einer Schadsoftware beabsichtigt. Das Gerät erwärmt sich, ist sehr langsam oder verbraucht sehr viel Energie, weil beispielsweise Videoaufnahmen in Echtzeit aufgezeichnet werden oder weil im Netzwerk verfügbare Dateien versendet werden.

Geringe Datenübertragungsraten Auch geringe Datenübertragungsraten können ein Anzeichen für ein Netzwerkproblem, schlechte Signalqualität, abgestürzte Apps oder das regelmäßige Synchronisieren sein – oder aber ein Hinweis darauf, dass Ihr Gerät ohne Ihr Wissen Daten herunterlädt oder versendet. Geringe Datenübertragungsraten können zudem darauf hindeuten, dass ein Gerät einen unrechtmäßigen Zugriffspunkt oder eine unrechtmäßige Funkzelle nutzt, die nicht so leistungsfähig ist wie das Original.

Überschreiten des Datenkontingents Wie bereits erörtert beschränkt ein Datenkontingent die Menge der Daten, die ein Gerät gemäß Mobilfunkvertrag übertragen darf. Ist das Kontingent ausgeschöpft, wird möglicherweise die Geschwindigkeit gedrosselt. Vielleicht hat der Benutzer während einer längeren Autofahrt über Spotify Musik gehört oder das Gerät versendet gestohlene Daten, die auf dem Gerät selbst oder im Netzwerk verfügbar sind.

Ungewollte Verbindungen

Ungewollte Netzwerkverbindungen, die über Mobilfunk, WLAN oder Bluetooth zustande kommen können, stellen ein erhebliches Sicherheitsrisiko dar. Ungewollte Mobilfunkverbindungen sind selten, weil die gewünschten Verbindungen im Mobiltelefon vom Anbieter vorkonfiguriert sind und gelegentlich aktualisiert werden. Es gibt jedoch ein Verfahren namens *Tower-spoofing* (Vortäuschen eines

Sendemasts), das an dieser Stelle erwähnt werden muss. Beim Tower-spoofing werden mittels entsprechender technischer Ausrüstung die Infrastruktur und der Sendemast eines Mobilfunkanbieters vorgetäuscht. Ein Mobiltelefon kann dadurch veranlasst werden, sich damit zu verbinden statt mit dem echten Sendemast. Dazu muss das Signal stärker als dasjenige des echten Sendemasts sein. Die hierfür erforderliche Ausrüstung kann außerdem dazu benutzt werden, beliebige Gespräche abzuhören, selbst wenn diese eigentlich über eine verschlüsselte Verbindung stattfinden, denn das Mobiltelefon kann durch ein paar Tricks dazu gebracht werden, die Verschlüsselung komplett zu deaktivieren und gewiefte Angreifer können sogar Malware auf dem Gerät installieren.

Nicht nur Hacker nutzen dieses Verfahren seit einigen Jahren, auch Strafverfolgungsbehörden sollen sich dem Vernehmen nach dieser Methode bedient haben. Seit 2010 gab es zahlreiche Gerichtsverfahren, die ein großes Medienecho fanden, bei denen es um die Zulässigkeit von Beweismaterial ging, das durch das Abhören von Mobilfunktelefonaten erlangt wurde. Medienberichten zufolge wurde dabei von mehreren staatlichen Strafverfolgungsbehörden ein Gerät namens »Stingray« (Stachelrochen) verwendet, um durch Einsatz von Tower-spoofing-Technik Telefonate von Verdächtigen abzuhören. Es gibt sogar eine Version namens »Dirtbox«, die für den Einsatz in Flugzeugen vorgesehen ist.

Hinweis

Der Großteil der Medienberichterstattung über Tower-spoofing bezieht sich auf US-Strafverfolgungsbehörden, die Stingray einsetzen. Ihnen könnten jedoch (aus einer Vielzahl von Gründen) überall auf der Welt bösartige Mobilfunk- oder WLAN-Netzwerke begegnen, die von Einzelpersonen, Unternehmen, Verbrecherbanden der organisierten Kriminalität oder Behörden betrieben werden.

Durch ungewollte WLAN-Verbindungen und Kopplungen mit Bluetooth-Geräten kann es nicht nur zu unerlaubtem Zugriff auf Daten kommen, sondern auch zu Datendiebstahl oder Datenmanipulation durch bösartige Angreifer. Konfigurieren Sie Ihr Gerät so, dass es sich nicht automatisch mit unbekannten WLAN-Netzwerken verbindet und dass die Kopplung von Bluetooth-Geräten standardmäßig nicht gestattet ist. Sie müssen sich dann zwar manuell mit vertrauenswürdigen WLAN-Netzwerken verbinden und Bluetooth-Geräte von Hand koppeln, aber das ist es wert. Diese Einstellungen können auch mittels der MDM-Software im Profil für das fragliche Gerät vorgenommen werden, sofern es zentral verwaltet wird.

Signalverlust oder schwaches Signal

Den Einfluss eines Signalverlusts oder eines schwachen Signals auf Akkulaufzeit, Energieverwaltung und die Ausführung von Apps habe ich bereits erläutert. Manchmal werden diese Probleme gar nicht bemerkt oder sie stellen nur ein kleines Ärgernis dar. Das Mobilfunksignal kann aber auch einer der wenigen Hinweise darauf sein, dass Ihr Gerät mit einer unrechtmäßigen Mobilfunkzelle kommuniziert.

Wenn Sie oder Ihre Benutzer sich in einem Gebiet aufhalten, in dem die Qualität des Mobilfunksignals hervorragend sein sollte (und normalerweise auch ist), sollten Sie misstrauisch werden, insbesondere dann, wenn mehrere Benutzer von Schwierigkeiten berichten. Erkundigen Sie sich beim Mobilfunkanbieter, ob es in dem Gebiet Probleme mit den Mobilfunkzellen gibt. Verwenden Sie einen Funkzellen-Analyzer und vergleichen Sie die vorliegenden Signale mit denen, die Sie früher ermittelt oder online recherchiert haben.

Wenn Benutzer berichten, dass die WLAN-Qualität in Bereichen schlecht ist, in denen sie vorher gut war, oder wenn Sie in einem Funkloch plötzlich ein starkes Signal eines WLANs mit der korrekten SSID empfangen, sollten Sie das überprüfen. Vielleicht wurde ein unrechtmäßiger Zugriffspunkt eingerichtet.

25.3.3 Unautorisierter Datenzugriff

Auf mobilen Geräten gespeicherte Daten zu schützen ist schwierig. Das Sicherheitspersonal würde einen Boten, der versucht, mit einem Desktop unterm Arm das Gebäude zu verlassen, vermutlich auf-

halten. Ein Smartphone in der Hosentasche würden sie aber wohl kaum bemerken. Und wenn doch, könnte der Bote immer noch glaubwürdig behaupten, dass er ein zusätzliches Smartphone für seine Arbeit benötigt, und seiner Wege gehen. Falls ich mein Smartphone beim Mittagessen versehentlich liegen lassen sollte, wäre es durchaus möglich, dass ich das erst bemerke, wenn ich mich abends auf den Weg zu meinem Auto mache. Normalerweise kann durch eine Gerätesperre oder durch Remote Wipe verhindert werden, dass unautorisierte Benutzer auf die auf dem mobilen Gerät gespeicherten Daten zugreifen – sofern das Löschen erfolgt, bevor das Gerät kompromittiert wird.

Daten können allerdings auch auf andere Weise in die falschen Hände geraten, etwa wenn sie sich auf entnehmbaren Speicherkarten befinden oder wenn die Systemeinstellungen des Geräts oder die Konfiguration anderer Apps dies zulässt. Die Inhalte entnehmbarer Speicherkarten sollten verschlüsselt werden, wenn sie sensible Daten enthalten, damit unautorisierte Personen nicht darauf zugreifen können, wenn die Karte dem Gerät entnommen wird. Die Geräte können durch Einstellungen für die Privatsphäre und die Sicherheit so konfiguriert werden, dass persönliche Daten geschützt sind. Vergleichbare Einstellungen gibt es auch für Apps, die den Zugriff auf persönliche Daten erlauben.

Ein eher offensichtliches Risiko für vernetzte Anwendungen mit Zugriff auf persönliche Daten ist die Möglichkeit, dass ein Programm einen Teil der Daten preisgibt, sei es absichtlich oder versehentlich. In manchen Fällen kann es schwierig sein, festzustellen, wo das Datenleck erfolgt. Wenn ein Angreifer Ihre bei Dropbox gespeicherte Steuererklärung nutzt, um in Ihrem Namen einen Kredit aufzunehmen, wo und wann sind die Daten dann verloren gegangen? Sie haben lokale Kopien auf dem Smartphone, auf dem Laptop und auf dem Desktop gespeichert, und die Dropbox enthält noch weitere Daten, die über ein Netzwerk übertragen wurden. Vielleicht hat der Angreifer die Daten aber auch direkt bei Ihrem Steuerberater gestohlen.

Entscheidend ist, dass verloren gegangene Daten ein Risiko darstellen, ein potenzielles Symptom für ein weiterhin bestehendes Sicherheitsproblem sind und möglicherweise einen Hinweis auf das Sicherheitsproblem geben. Eine vollständige Untersuchung aller Möglichkeiten, wie eine wichtige Datei in einer vernetzten Umgebung verloren gegangen sein könnte, kann man von einem CompTIA A+-Techniker nicht erwarten, man sollte jedoch die Chance nutzen, das Problem zu eskalieren oder es als kompromittiertes Kennwort abtun und den Benutzer auffordern, sein Kennwort zu ändern.

Wichtig

Für die auf mobilen Geräten wie Smartphones und Tablets gespeicherten persönlichen Daten besteht immer die Gefahr, dass sie verloren gehen und in die falschen Hände geraten. Die CompTIA bezeichnet das als »Verlust persönlicher Dateien/Daten«, man könnte das aber auch als »Das Kennwort taugt nichts und Sie haben Ihr Smartphone im Skiurlaub an der Hotelbar liegen gelassen« interpretieren. (Mir ist das zum Glück noch nie passiert.)

Unautorisierter Zugriff auf Benutzerkonten

Der unautorisierte Zugriff auf ein Benutzerkonto stellt nicht nur eine Gefahr für das betroffene Gerät dar, sondern auch für das Unternehmensnetzwerk, mit dem es verbunden ist. Wenn die Zugangsdaten zu einem Benutzerkonto bekannt werden oder ein Unbefugter das Gerät benutzen kann, ist das Unternehmensnetzwerk angreifbar. Wie bereits erwähnt, sollte man immer damit rechnen, dass jedes Gerät verloren gehen kann.

Damit VPN- und E-Mail-Zugang geschützt bleiben, sollten Benutzernamen und Kennwörter nicht gespeichert werden, um automatischen Zugang zu haben. Auf diese Weise kann nicht auf die Dienste zugegriffen werden (sofern nicht auch Zugangsdaten gestohlen wurden), wenn ein Gerät verloren geht oder gestohlen wird, weil noch immer eine Authentifizierung erforderlich ist. Der unautorisierte Zugriff auf ein Benutzerkonto gefährdet nicht nur die auf dem Gerät gespeicherten Daten, sondern auch die über das Netzwerk zugänglichen.

Wenn ein Gerät verloren gegangen ist, müssen Sie äußerst vorsichtig vorgehen. Betrachten Sie die beschriebenen Maßnahmen als etwas, das Sie schützt, bis ein Gerät als verloren gegangen gemeldet

wird. Sobald Sie davon wissen, sollten Sie die Zugangsdaten des Benutzers ändern. Denken Sie auch daran, dass kompromittierte Zugangsdaten für ein Benutzerkonto ein Hinweis darauf sein können, dass eines der Geräte des betroffenen Benutzers ebenfalls kompromittiert wurde und eine weiterhin bestehende Bedrohung für das Unternehmen darstellen könnte.

25.3.4 Unautorisierter Root-Zugriff

Zwecks Verbesserung der Sicherheit beschränken alle Betriebssysteme die Aktionen (wie die Installation von Programmen oder das Ändern von Einstellungen), die ein Benutzer normalerweise vornehmen kann. Diese Beschränkungen können umgangen werden. Für diesen Vorgang sind verschiedene Begriffe gebräuchlich, je nachdem, wie das Betriebssystem beschränkt und was dem Benutzer erlaubt ist. Das Gerät muss *gerootet* (Android) bzw. *gejailbreakt* (iOS) werden.

Wichtig

Im Grunde genommen sind die Begriffe austauschbar, aber bei iOS-Geräten spricht man von einem »Jailbreak«, während man diesen Vorgang bei Android- und Windows-Geräten als »Rooten« bezeichnet. Für das Entfernen der Zugriffsbeschränkungen sind beide Begriffe gebräuchlich.

Einen *Jailbreak* durchzuführen bedeutet, dass der Benutzer ein Programm auf dem Gerät installiert, das es ihm gestattet, Einstellungen vorzunehmen, deren Änderung eigentlich Apple vorbehalten sein sollte. Jailbreaking ermöglicht es dem Benutzer, normalerweise nicht erlaubte Software zu installieren, beispielsweise Apps, die nicht dem App-Store entstammen oder die sich nicht an Apples rechtliche Bedingungen oder Qualitätsanforderungen halten. Jailbreaking erlaubt es darüber hinaus, zusätzliche Funktionalitäten freizuschalten.

Das *Rooten* eines Android-Geräts ist eine vergleichbare Prozedur, die bewirkt, dass der Benutzer auch für die maschinennahen Funktionen vollständige administrative Rechte besitzt. Wie beim Jailbreak wird damit das Ziel verfolgt, sonst nicht ausführbare Software zu installieren und Funktionalitäten freizuschalten, die ohne Rooten nicht nutzbar wären. Zwar billigt keiner der großen Hersteller das Rooten seiner Geräte, da diese jedoch den Benutzern gehören, können sie, abgesehen von der Verweigerung von Garantieleistungen, praktisch nichts dagegen unternehmen.

Der entscheidende Punkt ist hier, dass beide Verfahren dem Benutzer zusätzlich Berechtigungen verschaffen, allerdings werden dadurch Schutzmaßnahmen ausgehebelt, die den Schaden begrenzen, den bösartige Apps auf dem Gerät anrichten können. Manche Dinge sind ohne das Entfernen der Beschränkungen mit einem Gerät schlicht und einfach nicht machbar, aber man sollte stets die Vorteile gegen das Risiko abwiegen, insbesondere wenn man entscheiden muss, ob gejailbreakte/gerootete Geräte im Netzwerk erlaubt sein sollen.

Hinweis

In Unternehmensnetzwerken kann die MDM-Software gejailbreakte/gerootete Geräte erkennen und blockieren.

Der Hersteller oder ein Diensteanbieter kann verhindern, dass ein Gerät die angebotenen Dienste nutzt, wenn ein gejailbreaktes/gerootetes Gerät erkannt wird. Es gibt auch unmittelbare Risiken: Ein fehlgeschlagener Versuch, ein Gerät zu jailbreaken oder zu rooten, kann es dauerhaft unbrauchbar machen (»Bricking«) oder zumindest unbenutzbar, bis eine vollständige Wiederherstellung anhand eines Backups erfolgt. Dabei wird die Jailbreaking/Rooting-Software entfernt.

Unautorisierte Nutzung der Ortungsdienste

Die Vorteile von GPS und Ortungsdiensten wurden bereits erwähnt, allerdings gibt es hier auch Sicherheitsbedenken. Die Einstellungen des Geräts erlauben es möglicherweise, den Aufenthaltsort

des Benutzers an Dritte zu übermitteln, manchmal ohne dessen Zustimmung oder Wissen. Um das zu verhindern, sollten Sie die GPS-Funktion und die Ortungsdienste am besten abschalten, wenn sie nicht in Gebrauch ist. Eine andere Möglichkeit besteht darin, das Gerät und die Geotracking verwendenden Apps so zu konfigurieren, dass keine unautorisierte Nutzung der Ortungsdienste erlaubt ist – wenn das machbar ist. Einige Apps oder bestimmte Features funktionieren ohne Geotracking überhaupt nicht (Abbildung 25.19).

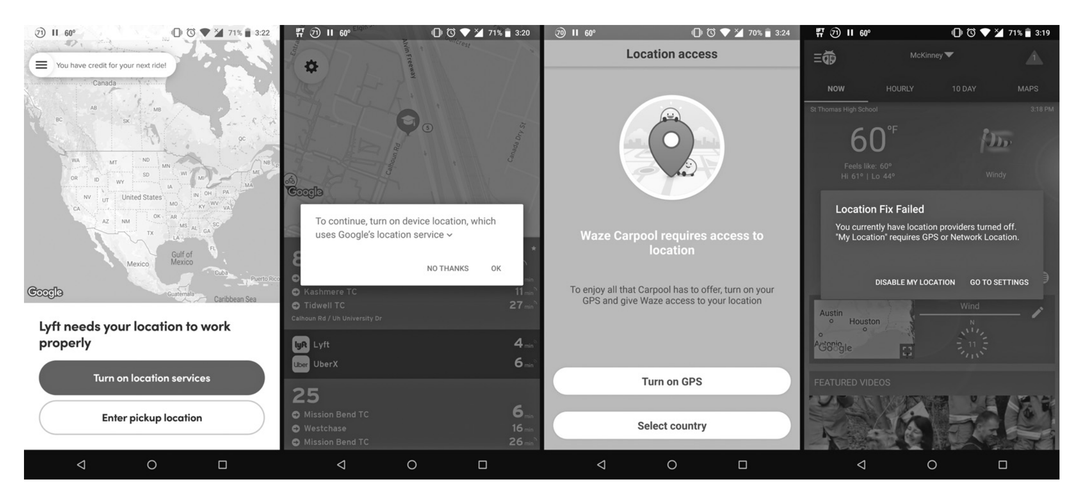


Abb. 25.19: Vier Android-Apps, die den Benutzer auffordern, die Ortungsdienste zu aktivieren

Denken Sie auch daran, dass GPS nicht die einzige Möglichkeit ist, den Aufenthaltsort zu bestimmen. Mobilfunknetze und WLANs können ebenfalls zur Ortung herangezogen werden, wenngleich die so ermittelte Position nicht so präzise ist wie bei GPS. Einige der im Abschnitt *Angriffe über das Netzwerk* beschriebenen Methoden können ebenfalls zur Ortung eines Geräts eingesetzt werden.

Ein Unternehmen kann ein Geotracking der Mitarbeiter durchführen und registrieren, wenn sie ein bestimmtes Gebiet betreten oder verlassen, ein Vorgang, der als *Geofencing* bezeichnet wird. Den Angestellten dürfte das weniger gut gefallen, denn sie empfinden das als eine Form der Arbeitsplatzüberwachung und wehren sich womöglich dagegen. Verärgerte Mitarbeiter lassen ihre Geräte beim Verlassen des Arbeitsplatzes einfach auf dem Schreibtisch liegen. Oder sie suchen sich rechtlichen Beistand und ziehen eine Klage gegen den Arbeitgeber wegen Verletzung der Privatsphäre in Betracht. Es ist zweifelsohne am besten, die rechtlichen Fragen und die Vor- und Nachteile einer Mitarbeiterüberwachung vorab zu klären.

25.3.5 Unautorisierte Aktivierung von Kamera und Mikrofon

Die Funktionen einer App, Malware und unautorisierte Netzwerkverbindungen können potenziell dazu verwendet werden, verschiedene Funktionalitäten eines Smartphones oder Tablets aus der Ferne zu aktivieren (oder zu deaktivieren!). Eingebaute Kameras und Mikrofone bereiten hier die größten Sorgen. Ihre Aktivierung würde es einem bösartigen Angreifer erlauben, alle in der Nähe befindlichen Personen auszuspionieren.

Hinweis

Um das zu verhindern, sollte der Zugriff auf Kamera und Mikrofon in den einzelnen Apps und im Betriebssystem beschränkt werden (sofern das möglich ist). Folgen Sie außerdem den vorhin beschriebenen Schritten zur Verhinderung unautorisierter Netzwerkverbindungen und setzen Sie eine Anti-Malware-Software ein. Auch Apps von vertrauenswürdigen Entwicklern, wie die iOS-Apps mit Zugriffsrechten auf

die Kamera in Abbildung 25.20 können ein Risiko darstellen, denn jede Schwachstelle in einer vernetzten App mit diesen Berechtigungen könnte einem Angreifer ein Ausspionieren ermöglichen.

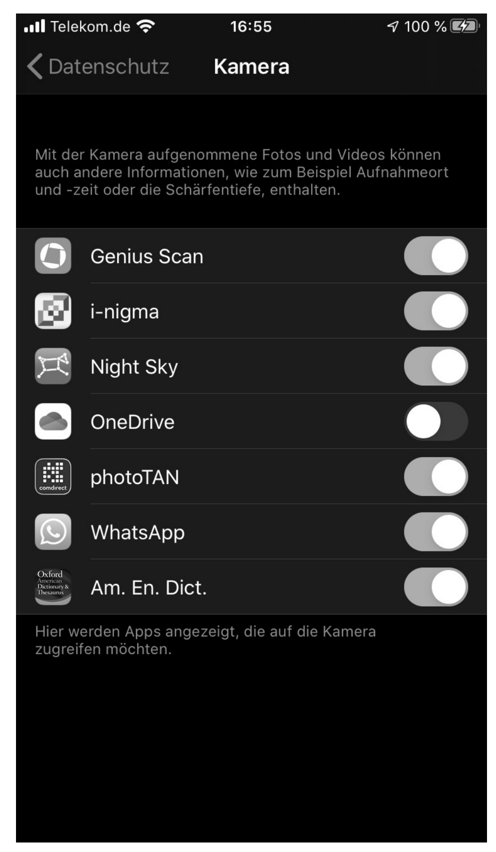


Abb. 25.20: Apps mit Zugriffsrechten auf die Kamera

25.4 Wiederholung

25.4.1 Fragen

1. Nachdem Sie fünf Minuten lang mit einem extrem langsamen Gerät gekämpft haben, gelingt es Ihnen schließlich, die schuldige App zu beenden. Was sollten Sie am besten als Nächstes tun?
   - **A.** Die App erneut starten und hoffen, dass sie nicht abstürzt
   - **B.** Die App deinstallieren und nach Ersatz suchen
   - **C.** Warmstart durchführen und prüfen, ob die App danach ordnungsgemäß funktioniert
   - **D.** Alle laufenden Apps beenden und die Anwendung erneut öffnen, um zu prüfen, ob sie wieder abstürzt
2. Was könnte der Grund dafür sein, dass ein Smartphone oder Tablet langsam läuft?
   - **A.** Fehlerhafte Kalibrierung
   - **B.** Zu langsames RAM

C. Zu wenig Speicherplatz
D. Falsche Programmversion

3. Johannas GPS-Karten-App zeigt die Fehlermeldung »GPS-Koordinaten nicht verfügbar« an. Was sollte sie als Erstes ausprobieren?
   A. Eine andere GPS-App benutzen
   B. GPS deaktivieren und dann wieder aktivieren
   C. Sich an einen Ort begeben, an dem ein GPS-Signal empfangen werden kann
   D. Firmware des Geräts aktualisieren
4. Sie haben Ihr iPhone verloren. Wie versuchen Sie es wiederzufinden?
   A. iTunes
   B. iFind
   C. Ortungsdienste
   D. iCloud
5. Frank möchte auf seinem Desktop-PC *World of Warcraft* spielen. Er meldet sich mit seinem Kennwort an und wird aufgefordert, einen von einer Authentifizierungs-App auf seinem Android-Smartphone erzeugten Code einzugeben. Hierbei handelt es sich um ein Beispiel für:
   A. Mehrfaktor-Authentifizierung
   B. Faktor-Authentifizierung
   C. Mehrfaktor-Autorisierung
   D. Faktor-Autorisierung
6. Ein Jailbreak eines iPhones ermöglicht den Zugriff auf
   A. das Administrator-Benutzerkonto
   B. das Root-Benutzerkonto
   C. den Ordner `/bin`
   D. das System-BIOS
7. Wie lassen sich die Daten auf einer entnehmbaren Speicherkarte am besten schützen?
   A. Verschlüsseln
   B. Sperren
   C. Entfernen, wenn sie nicht benötigt werden
   D. Formatieren
8. Welches Betriebssystem für mobile Geräte benötigt eine Firewall von einem Drittanbieter?
   A. Android
   B. macOS
   C. Windows Mobile
   D. iOS
9. Wie nennt man es, wenn Benutzer in einer Unternehmensumgebung ihre eigenen Geräte verwenden?
   A. Importieren
   B. CMYK
   C. Bereitstellen
   D. BYOD
10. Was leisten App-Scanner?

A. QR-Codes und Barcodes nach verborgenen Codes durchsuchen
B. Ein- und ausgehenden Datenverkehr einer App auf verdächtiges Verhalten überprüfen
C. Analyse der Berechtigungen installierter Apps und Hervorheben von Sicherheitsrisiken
D. Analyse von WLAN-Signalen zwecks Identifizierung unrechtmäßiger Zugangspunkte

25.4.2 Antworten

1. **C.** Nachdem Sie fünf Minuten lang mit einem extrem langsamen Gerät gekämpft haben, sollten Sie einen Warmstart durchführen und prüfen, ob die App danach ordnungsgemäß funktioniert.
2. **C.** Zu wenig Speicherplatz könnte der Grund dafür sein, dass ein Smartphone oder Tablet langsam läuft.
3. **C.** Johanna sollte sich an einen Ort begeben, an dem sie ein GPS-Signal empfangen kann.
4. **D.** Apples iPhone verwendet die iCloud-Funktion MEIN IPHONE SUCHEN.
5. **A.** Die Verwendung von Kennwort und Sicherheitscode ist ein Beispiel für Mehrfaktor-Authentifizierung.
6. **B.** Ein Jailbreak ermöglicht den Zugriff auf das Root-Benutzerkonto.
7. **A.** Am besten lassen sich die Daten auf einer entnehmbaren Speicherkarte durch eine Verschlüsselung schützen.
8. **A.** Nur Android benötigt eine Firewall von einem Drittanbieter.
9. **D.** Wenn Benutzer in einer Unternehmensumgebung ihre eigenen Geräte verwenden, wird das als *Bring Your Own Device* (BYOD) bezeichnet.
10. **C.** App-Scanner analysieren die Berechtigungen installierter Apps, um Sicherheitsrisiken hervorzuheben.

Drucker und Multifunktionsgeräte 26

Themen in diesem Kapitel:

- Aktuelle Technologien von Druckern und Multifunktionsgeräten
- Die Funktionsweise des Laserdruckers
- Installation und Konfiguration von Druckern und Multifunktionsgeräten
- Grundlegende Probleme bei der Verwendung von Druckern und Multifunktionsgeräten erkennen und beheben

Trotz des ganzen Geredes über das »papierlose Büro« bleiben Drucker ein unverzichtbarer Teil des typischen Büros. In vielen Fällen dienen PCs ausschließlich dem Zweck, Ausdrucke bzw. Dokumente auf Papier zu produzieren. Viele Anwender arbeiten trotz zunehmender Verbreitung tragbarer Geräte einfach lieber mit Ausdrucken. Und auch die Programmierer bedienen sich der Metaphern aus dem Büroalltag und verwenden in ihren Anwendungen Begriffe wie »Seite«, »Arbeitsmappe« und »Ordner«.

Früher gab es in einem typischen Büro eine Reihe verschiedener elektronischer und mechanischer Geräte, die mit Dokumenten aus Papier jeweils nur eine einzige Aufgabe erfüllen konnten: Drucker, Kopierer, Scanner oder Faxgeräte. Seit den 1990er-Jahren versuchten die Hersteller, mehrere dieser Funktionen (zumeist Drucken und Scannen) in *Multifunktionsgeräten* (Mufus) zu vereinen. Anfangs erledigten derartige Geräte keine der Funktionen, die sie beherrschten, besonders gut, allerdings erledigen die technisch inzwischen ausgereiften Multifunktionsgeräte ihre vielen Aufgaben heutzutage durchaus gut.

Im Rahmen der CompTIA A+-Zertifizierung wird der Bereich des Druckens stark betont. Von Ihnen wird ein hohes Maß an Kenntnissen der Funktionen und Komponenten, der Wartung und der Reparatur aller Drucker und Multifunktionsgeräte erwartet.

Dieses Kapitel stellt die verschiedenen Drucker- und Scanner-Varianten vor und erläutert dann die Funktionsweise des Laserdruckers. Danach geht es um die Installation von Multifunktionsgeräten auf einem typischen PC und schließlich um die Fehlerbehebung.

1001

26.1 Komponenten und Technologien von Druckern und Multifunktionsgeräten

Die heutzutage überall vorhandenen Multifunktionsgeräte stehen meist auf einem Schreibtisch oder in einem Regal und sind sich äußerlich oft ziemlich ähnlich. Wenn man an ein Multifunktionsgerät denkt, stellt man sich im Allgemeinen ein kleines Gerät vor, das auf dem Schreibtisch steht, an einem in der Nähe befindlichen Computer angeschlossen ist, und mehrere Funktionen in sich vereint. Für gewöhnlich kann man es zum Drucken, Scannen, Kopieren und Faxen verwenden (Abbildung 26.1).

Tatsächlich sind diese kleinen Tischgeräte Nachfahren des Schreibtischdruckers und repräsentieren das untere Ende des Marktspektrums. Geräte am oberen Ende des Spektrums sehen eher wie Kopierer oder sogar wie kleine Druckmaschinen aus. Trotz des unterschiedlichen Aussehens dieser High-End-Geräte verwenden sie doch die gleichen Komponenten, nämlich einen Drucker und einen Scan-

ner, wie ihre kleineren Verwandten, die Ihnen bereits vertraut sind. Die Geräte am oberen Marktspektrum sind vor allem schneller und stabiler, können größere Kapazitäten verarbeiten, und verfügen über Funktionen zur Handhabung der ausgegebenen Dokumente, wie etwa Sortierung, Heftung, Bindung usw.



Abb. 26.1: Multifunktionsgerät: Drucker, Scanner, Fax, Kopierer und iPod-Andockstation

Weil Multifunktionsgeräte so verschiedenartig sind, sehen wir uns die einzelnen Komponenten und Technologien, die hier zu finden sind, der Reihe nach genauer an. Die einzelnen Komponenten eines Multifunktionsgeräts können Ihnen durchaus auch in Form eigenständiger Geräte begegnen. Ich habe in diesem Abschnitt 3-D-Drucker hinzugefügt. Diese werden Ihnen allerdings nur als eigenständige Geräte begegnen, nicht als Mufus.

26.1.1 Drucker

Kaum eine andere Hardwarekomponente für Computersysteme ist in größerer Vielfalt, in mehr verschiedenen Konfigurationen und mit mehr unterschiedlichen Merkmalen erhältlich als der Drucker. Und auch die Preise sind von entsprechender Bandbreite. Was ein Drucker kann, ist weitgehend von der verwendeten Druckertechnologie abhängig und damit davon, wie der Ausdruck zu Papier gebracht wird. Moderne Drucker lassen sich in mehrere allgemeine Kategorien einteilen, zu denen Anschlagdrucker, Tintenstrahldrucker, Farbsublimationsdrucker, Thermodrucker, Laserdrucker, 3-D-Drucker und virtuelle Drucker zählen.

Anschlagdrucker

Drucker, die das Druckbild dadurch erzeugen, dass ein Farbband physisch gegen die Oberfläche des Papiers gedrückt wird, werden *Anschlagdrucker* genannt. *Typenraddrucker* (bei denen es sich im Wesentlichen um eine an den PC und nicht direkt an eine Tastatur angeschlossene elektrische Schreibmaschine handelt) sind weitgehend von der Bildfläche verschwunden. Die ihnen verwandten *Matrixdrucker* (Nadeldrucker) verrichten aber in vielen Büros weiterhin ihren Dienst. Zwar sind entsprechende Geräte beinahe vollständig aus den Regalen der Händler verschwunden, da sie nicht die vom Heimanwender bei niedrigen Preisen erforderliche Qualität und Flexibilität bieten können, aber im harten Büroeinsatz sind Nadeldrucker auch heute noch recht weit verbreitet. Dafür gibt es zwei Gründe: Die installierte Basis ist im Geschäftsbereich immer noch groß und sie eignen sich für das Bedrucken von Durchschlagformularen, da sie das Papier tatsächlich mechanisch bedrucken. Anschlagdrucker sind meist recht langsam und laut. Sie liefern aber akzeptable Ergebnisse, wenn Geschwindigkeit,

Druckqualität und Flexibilität nicht so entscheidend sind. Rechner, die für das Bedrucken von Mehrfachformularen eingesetzt werden, wie z.B. am Ort des Verkaufs (POS – *Point of Sale*), und Rechnungen, Quittungen oder Belege in mehreren Kopien erstellen müssen, bilden in erster Linie den Markt für neue Matrixdrucker, auch wenn bis heute viele ältere Matrixdrucker weiterhin ihren Dienst verrichten.

Matrixdrucker (Abbildung 26.2) arbeiten mit gitterförmig angeordneten, winzigen *Nadeln*, die auf das Druckerfarbband treffen und das Schriftbild auf dem Papier erzeugen. Das Bauteil, das die Nadeln enthält, wird *Druckkopf* genannt. Matrixdrucker arbeiten entweder mit neun oder 24 Nadeln und behandeln alle Seiten wie aus einzelnen Punkten bestehende Rasterbilder. Matrixdrucker mit neun Nadeln bieten nur Entwurfsqualität (draft quality), während bei 24-Nadel-Druckern von Briefqualität (letter quality) oder annähernder Briefqualität (near letter quality) gesprochen wird. Das BIOS des Druckers (entweder im Drucker eingebaut oder in einen Druckertreiber integriert) interpretiert das Rasterbild auf dieselbe Weise wie der Bildschirm und setzt das Bild aus einzelnen Punkten (dots) zusammen. Je mehr Nadeln, desto höher natürlich die Auflösung. Abbildung 26.3 zeigt die üblichen Komponenten eines Matrixdruckers. Viele Matrixdrucker verwenden Endlospapier mit seitlichen Lochstreifen, in die Zapfen aus Metall oder Kunststoff greifen, um es zu transportieren. Hierbei wird von Traktortransport gesprochen, weil die Radzähne an die Räder von Traktoren erinnern.



Abb. 26.2: Ein Epson-FX-880+-Matrixdrucker (Foto mit freundlicher Genehmigung von Epson)

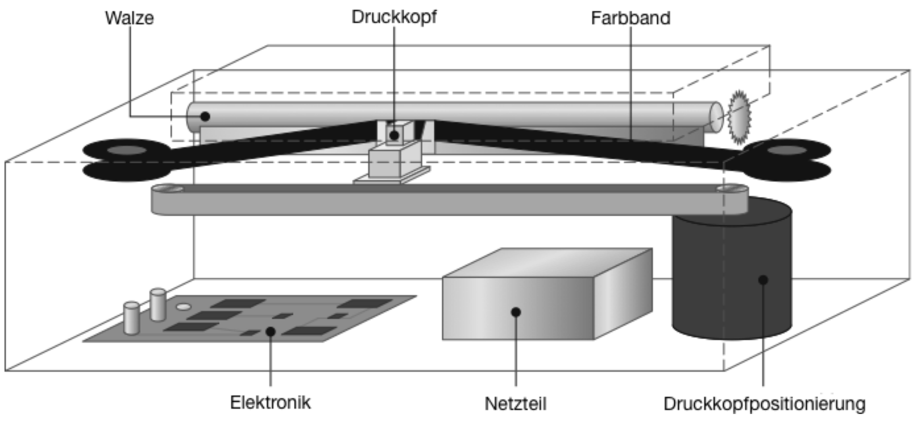


Abb. 26.3: Das Innere eines Matrixdruckers

Tintenstrahldrucker

Tintenstrahldrucker (Abbildung 26.4) sind relativ einfache Geräte, die aus dem Druckkopf-Mechanismus, der unterstützenden Elektronik, einem Mechanismus zur Bewegung des Druckkopfs und dem Transportmechanismus bestehen, der das Papier einzieht, befördert und auswirft (Abbildung 26.5).



Abb. 26.4: Typischer Tintenstrahldrucker

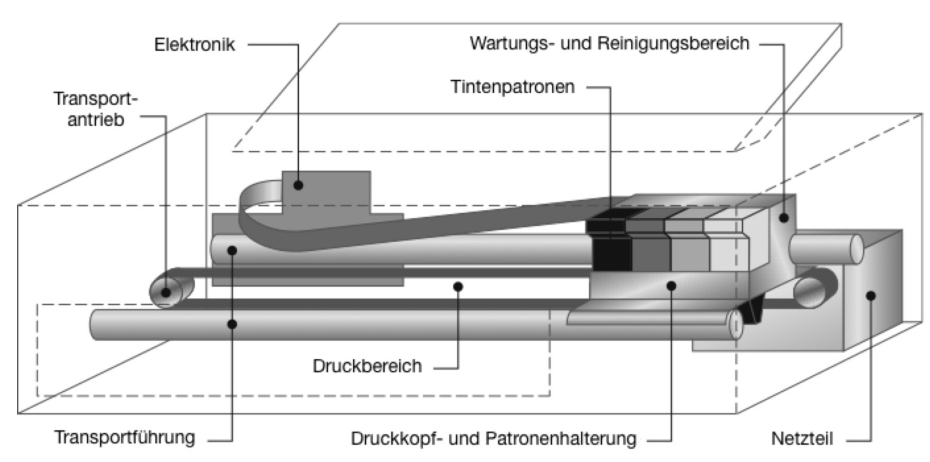


Abb. 26.5: Das Innere eines Tintenstrahldruckers

> **Wichtig**
>
> Manche Drucker verwenden eine *Duplex-Einheit*, die es dem Drucker erlaubt, automatisch beide Seiten des Papiers zu bedrucken. Bei einigen Geräten ist dieser Mechanismus eingebaut, bei anderen handelt es sich um zusätzliche Hardware, die das Papier für den Drucker wendet.

Tintenstrahldrucker schießen Tinte durch winzige Röhrchen bzw. *Düsen* auf das Papier. Bei den meisten Tintenstrahldruckern wird die Tinte durch Hitze auf das Papier aufgebracht (einige arbeiten mit

mechanischen Verfahren). Die Tinte wird von winzigen Widerständen oder elektrisch leitenden Plättchen am Ende der einzelnen Röhrchen erhitzt. Die Tinte wird von diesen Widerständen oder Plättchen buchstäblich »aufgekocht«, sodass winzige Luftbläschen entstehen, die dafür sorgen, dass die Tintentröpfchen auf das Papier geschleudert werden und einzelne Bildpunkte erzeugen (Abbildung 26.6).

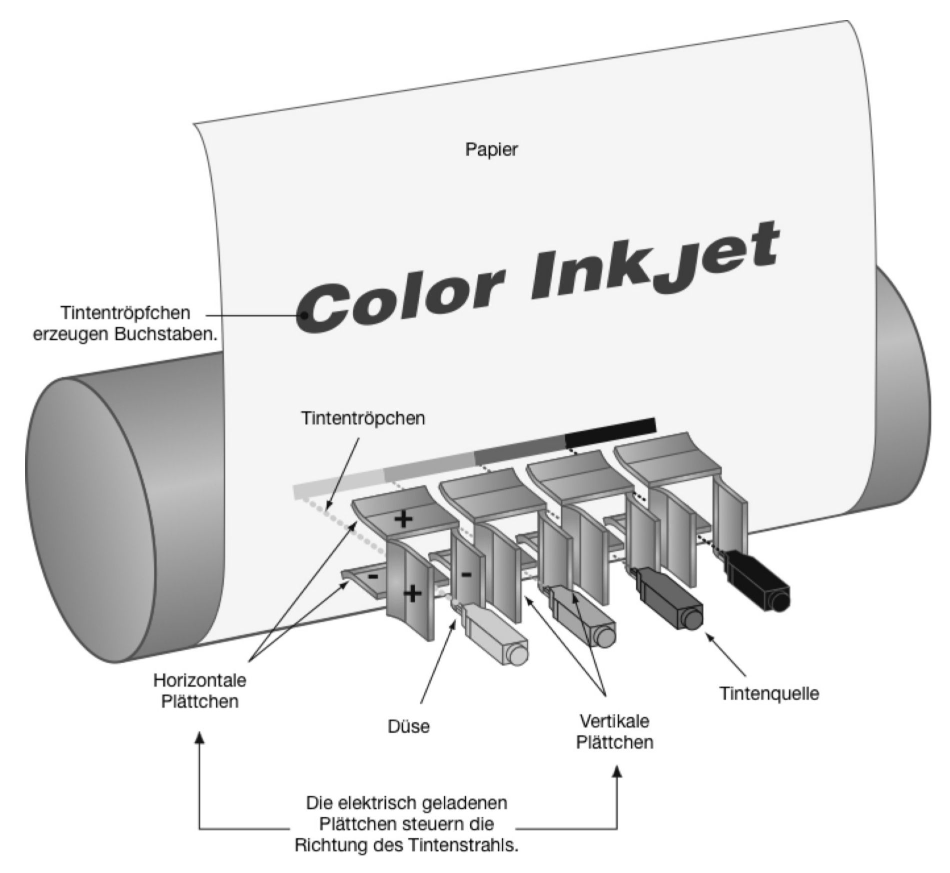


Abb. 26.6: Detailansicht eines Tintenstrahldruckkopfs

Die Tinte wird in speziellen kleinen Behältern vorrätig gehalten, die *Tintenpatronen* genannt werden. Ältere Tintenstrahldrucker hatten zwei Patronen: eine für schwarze Tinte und eine weitere für farbige Tinte. Die Farbpatrone hatte separate Fächer für Zyan, Magenta und Gelb, um die Farben unter Verwendung der CMYK-Methode (mehr dazu später in diesem Kapitel) zu drucken. Wenn in der Farbpatrone eine dieser Farben ausging, musste man eine völlig neue Farbpatrone kaufen oder komplizierte Füllwerkzeuge benutzen.

Die Druckerhersteller begannen, die farbigen Tinten in drei separaten Patronen unterzubringen, sodass die Drucker schließlich vier Patronen hatten: eine für jede Farbe und eine vierte für Schwarz (Abbildung 26.7). Das war nicht nur preiswerter für den Benutzer, sondern sorgte auch für qualitativ bessere Ausdrucke. Heute findet man auch Farbtintenstrahler mit sechs, acht oder mehr Farbpatronen. Neben den vier CMYK-Basistinten gibt es noch weitere Patronen z.B. für Grün, Blau, Grau, Hellblau, Hellrot usw. Normalerweise gilt, je mehr Tintenpatronen ein Drucker verwendet, desto höher ist die Qualität des ausgedruckten Bildes – und umso teurer ist der Drucker.



Abb. 26.7: Patronen für Tintenstrahldrucker

In den letzten Jahren haben Hersteller wie Epson und Canon Tintenstrahldrucker mit nachfüllbaren Tintenpatronen vorgestellt und damit das Geschäftsmodell für Drucker völlig verändert. Anstatt preiswerte Drucker anzubieten und mit dem Verkauf von Einweg-Tintenpatronen Geld zu verdienen, können Privat- und Geschäftskunden jetzt ohne weitere Umstände (und ohne sich wegen der Einweg-Patronen schuldig zu fühlen) viel mehr Seiten in Farbe drucken. Die Drucker sind zwar erheblich teurer geworden (ca. 350 bis 450 Euro statt etwa 60 bis 110 Euro), sind aber mit einem Tintenvorrat ausgestattet, der für mehrere Jahre reichen sollte. Jetzt wird es kunterbunt!

Bei der *Druckauflösung* (wie fein bzw. dicht die Tinte auf das Papier aufgetragen werden kann) und der *Druckgeschwindigkeit* handelt es sich um die beiden wichtigsten Merkmale von Tintenstrahldruckern. Die horizontale und vertikale Auflösung wird in *dots per inch* (dpi – Punkte pro Zoll) angegeben, wie z.B. 2400 x 600 dpi. Höhere Werte weisen darauf hin, dass die Abstände zwischen den einzelnen Druckpunkten auf dem Blatt kleiner sind, was zu einem besseren Aussehen der gedruckten Dokumente führt. Die Auflösung ist beim Ausdruck komplexer Bilder, wie z.B. Farbfotos, und beim Erstellen von Druckvorlagen, die vervielfältigt werden und entsprechend gut aussehen sollen, besonders wichtig. Die *Druckgeschwindigkeit* wird in Seiten pro Minute (ppm – *pages per minute*) angegeben. Bei Farbdruckern werden normalerweise zwei Geschwindigkeiten angegeben, eine (die höhere) für Schwarz-Weiß-Druck und die zweite für farbige Ausdrucke.

Wichtig

Die Druckauflösung wird in dpi (dots per inch) und die Druckgeschwindigkeit in ppm (pages per minute) angegeben.

Ein weiteres Merkmal von Tintenstrahldruckern ist, dass sie eine Reihe verschiedener Druckmedien unterstützen. Mit einem Tintenstrahldrucker können Sie auf verschiedene matte oder glänzende Fotopapiere oder auf Folie drucken, ebenso wie auf andere spezielle Medien. Einige Drucker können direkt auf speziell beschichtete optische Datenträger drucken oder sogar auf Stoff. Sie könnten also ein T-Shirt durch Ihren Drucker laufen lassen und ihm Ihr ganz eigenes Motto aufdrucken (etwa »Ich bin CompTIA A+-zertifiziert!«). Und auch die Tinten sind im Laufe der Jahre besser geworden und bieten heute höhere Qualität und sind langlebiger als je zuvor. Während ältere Tinten verschmierten, wenn das Papier feucht wurde, oder innerhalb kurzer Zeit verblassten, sind moderne Tinten relativ schmiersicher und bieten Archivqualität – einige Tinten von Epson beispielsweise sind auf eine Lebensdauer von 200 Jahren ausgelegt.

Tipp: Seiten pro Minute und der Preis

Die Druckgeschwindigkeit ist für den Preis eines Druckers mit ausschlaggebend, wie sich leicht zeigen lässt:

1. Starten Sie Ihren Webbrowser und besuchen die Websites von Hewlett-Packard (`http://www.hp.com`), Canon (`http://www.canon.com`), Epson (`http://www.epson.com`), Brother (`http://www.brother.com`) oder Samsung (`http://www.samsung.com`). Diese fünf Hersteller liefern den Löwenanteil der heutzutage auf dem Markt erhältlichen Drucker.
2. Wählen Sie eine Drucktechnologie aus und überprüfen Sie die Preise, vom preiswertesten Drucker bis zum teuersten. Suchen Sie dann nach Druckern mit gleicher Auflösung, aber höherer Druckgeschwindigkeit.
3. Vergleichen Sie die Preise und überprüfen Sie, wie die Seitenzahl pro Minute den Preis zweier ansonsten gleichwertiger Drucker beeinflusst.

Farbsublimationsdrucker

Der Begriff *Sublimation* steht für einen Prozess, bei dem etwas von einem festen in einen gasförmigen Zustand übergeht (oder umgekehrt). Dieser Vorgang beschreibt die Arbeitsweise des Farbsublimationsdrucks, der manchmal auch Thermofarbtransferdruck genannt wird. Bei den »Tinten« ist entsprechend von Festtinten- oder Feststofftinten die Rede. *Farbsublimationsdrucker* werden vorwiegend für den Druck von Fotos, High-End-Desktop-Publishing, medizinische und wissenschaftliche Drucke oder andere Anwendungen genutzt, bei denen feine Details und satte Farben wichtiger als Kosten und Geschwindigkeit sind. Kleinere, spezialisierte, sogenannte *Fotodrucker* arbeiten mit der Sublimationstechnik und sind deutlich preiswerter als ihre großen Kollegen.

Beim Farbsublimationsdruck handelt es sich um ein Beispiel des CMYK-Farbdrucks (**c**yan, **m**agenta, **y**ellow, blac**k**). Dabei wird meist eine wärmeempfindliche Rolle mit Kunststofffolie verwendet, auf der es Abschnitte in Seitengröße gibt, in denen die jeweiligen Farben aufgetragen sind. Teilweise gibt es Abschnitte für Zyan, Magenta und Gelb, teilweise kommt aber auch ein schwarzer Abschnitt hinzu. Ein Druckkopf enthält Tausende von Heizelementen, deren Temperatur exakt gesteuert werden kann und die über die Kunststofffolie bewegt werden. Die Farbstoffe werden durch das Erwärmen gasförmig und verbinden sich, bevor sie wieder abkühlen und in ihren festen Zustand übergehen, mit dem unter der Rolle durchgeführten, speziell beschichteten Papier. Bei diesem Prozess ist für die einzelnen Farben jeweils ein eigener Druckdurchgang erforderlich. Einige Drucker arbeiten zudem mit einem abschließenden Durchgang, bei dem auf die Seite z.B. eine Schutzschicht aufgetragen wird (Laminierung). Abbildung 26.8 verdeutlicht die Arbeitsweise von Farbsublimationsdruckern.

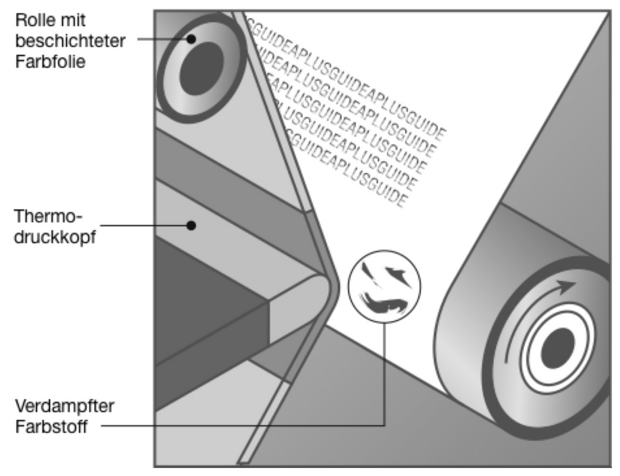


Abb. 26.8: Farbsublimationsdruck

Das Farbsublimationsverfahren erzeugt im Druck *kontinuierliche Farbtöne*. Jeder einzelne Bildpunkt entsteht durch Mischen verschiedener Farbstoffe. Damit unterscheidet sich dieses Verfahren von den gerasterten Bildern der anderen Drucktechnologien, bei denen über einfarbige, dicht nebeneinander platzierte Druckpunkte Farbverläufe simuliert werden (Dithering). Farbsublimationsdrucker erzeugen qualitativ hochwertige Farbdrucke, die mit den Ergebnissen professioneller Fotolabore konkurrieren können.

Thermodrucker

Thermodrucker verwenden einen beheizten Druckkopf, um auf Spezial- oder Normalpapier hochwertige Bilder aufzubringen. Es gibt zwei Arten: *Thermodirekt-Drucker* und *Thermowachsdrucker*. Thermodirekt-Drucker arbeiten mit einem erhitzten Druckkopf, der die Punkte in die Oberfläche eines speziellen wärmeempfindlichen Papiers brennt. Wenn Sie sich noch an die erste Generation von Faxgeräten erinnern können, dann sind Sie bereits mit dieser Art von Druckern vertraut. Derartige Drucker werden auch heute noch in vielen Kaufhäusern als Belegdrucker genutzt und besitzen oft einen Mechanismus zum Abschneiden des Belegs.

Thermowachsdrucker arbeiten ähnlich wie Farbsublimationsdrucker, benutzen aber keine Folienrollen mit eingebetteten Farbstoffen, sondern Folien, die mit farbigem Wachs beschichtet sind. Der Thermodruckkopf wird dabei über die Folie geführt und verschmilzt das Wachs mit dem Papier. Für Thermowachsdrucker muss kein spezielles Papier wie für Farbsublimationsdrucker verwendet werden, wodurch sie flexibler und im Einsatz etwas preiswerter sind. Die Qualität des Ausdrucks ist aber weniger gut, da die Farbverläufe durch Dithering erzeugt werden.

Laserdrucker

Laserdrucker erzeugen mit einem elektrooptischen Verfahren qualitativ hochwertige Text- und Grafikausdrucke und arbeiten dabei sehr schnell. Abbildung 26.9 zeigt einen typischen Laserdrucker. Die Funktion der Laserdrucker stützt sich auf die Lichtleitfähigkeit bestimmter organischer Verbindungen. Lichtleitfähigkeit bedeutet, dass diese Partikel Elektrizität leiten, wenn sie einer Bestrahlung durch Licht ausgesetzt werden. Bei Laserdruckern werden Laser als Lichtquelle eingesetzt, weil diese äußerst präzise arbeiten. Einige preiswertere Drucker verwenden stattdessen LED-Felder.



Abb. 26.9: Typischer Laserdrucker

Die ersten Laserdrucker konnten nur Schwarz-Weiß-Bilder erzeugen. Heute sind zwar auch Farblaserdrucker erhältlich, aber es werden weiterhin vorwiegend Schwarz-Weiß-Laserdrucker hergestellt. Ein

Farblaser kann komplexe Vollfarbbilder wie beispielsweise Fotos ausdrucken, aber hauptsächlich werden sie genutzt, um sogenannte Schmuckfarben auszudrucken – beispielsweise attraktive Überschriften, Zeilen, Diagramme oder andere grafische Elemente, die eine sonst einfach gedruckte Präsentation verschönern. Hierbei können auch Farben verwendet werden, die sich mit den Grundfarben nicht erzeugen lassen, etwa Gold-, Silber- oder Leuchtfarben.

Hinweis: Versteckte Kosten

Einige Drucker haben einen sehr viel höheren Verbrauch, z.B. an Tinte, als andere, deshalb bewertet die Branche Drucker im Hinblick auf Kosten pro Seite. Bei einem billigen Drucker (Laser oder Tintenstrahler) kostet eine Seite vielleicht 4 Cent, während ein teurer Drucker Kosten von mehr als 20 Cent pro Seite verursachen kann – ein riesiger Unterschied, wenn Sie sehr viel drucken.

Die versteckten Kosten sind vor allem bei Tintenstrahldruckern im Preisbereich unterhalb von 100 Euro sehr unangenehm. Ihre niedrigen Preise locken häufig Kunden an, die dann feststellen, dass sie immense Verbrauchskosten verursachen. Ein einziger Satz farbiger und schwarzer Tintenstrahlpatronen kostet manchmal mehr als ein neuer Drucker!

In den CompTIA A+-Zertifizierungsprüfungen wird großer Wert auf die Besonderheiten des Druckprozesses von Laserdruckern gelegt, deshalb sollten Sie sich mit einem Laserdrucker auskennen. Jetzt werden wir uns mit den vielen Komponenten eines Laserdruckers und ihren Funktionen beschäftigen (Abbildung 26.10).

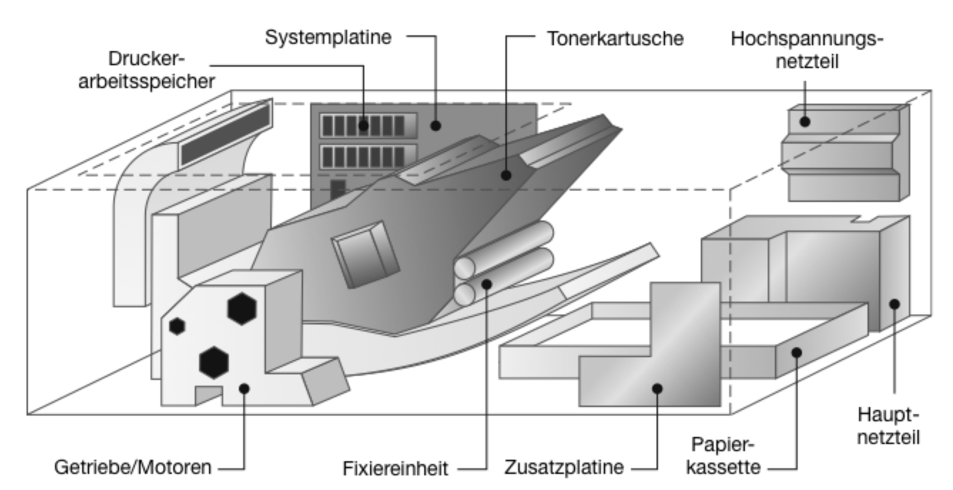


Abb. 26.10: Komponenten im Inneren eines Laserdruckers

Die Tonerkartusche In einem Laserdrucker versorgt die *Tonerkartusche* (Abbildung 26.11) den Drucker mit dem Toner, der auf das Papier aufgetragen wird und dort das Bild erzeugt. Zur Verringerung der Wartungskosten befinden sich viele Komponenten (insbesondere jene, die dem stärksten Verschleiß unterliegen) des Laserdruckers ebenfalls in der Tonerkartusche. Dadurch wird zwar der Austausch *einzelner* Komponenten nahezu unmöglich, dieser ist aber auch kaum noch erforderlich, da jene Komponenten, deren Ausfallwahrscheinlichkeit am höchsten ist, ohnehin jeweils beim Wechsel der Kartusche ersetzt werden.

Hinweis

Bei Farblaserdruckern gibt es vier Tonerkartuschen für die vier CMYK-Farben.



Abb. 26.11: Tonerkartusche eines Laserdruckers

Belichtungstrommel Bei der *Belichtungstrommel* (eine andere Bezeichnung lautet *Bildtrommel*) handelt es sich um einen Aluminiumzylinder, der mit lichtempfindlichen Materialien beschichtet ist. Die Trommel selbst wird über das Netzteil geerdet, die Beschichtung aber nicht. Wenn Licht auf diese Partikel trifft, wird deren elektrische Ladung über den geerdeten Zylinder abgeführt.

Löschlampe Die *Löschlampe* setzt die gesamte Oberfläche der lichtempfindlichen Trommel einer Bestrahlung durch Licht aus und sorgt so dafür, dass die lichtempfindliche Beschichtung leitend wird. Alle in den Partikeln vorhandenen elektrischen Ladungen fließen über die geerdete Trommel ab, wodurch die Teilchen an der Oberfläche elektrisch neutral werden.

Koronadraht/Ladewalze Der *Koronadraht* (oder bei neueren Geräten die *Ladewalze*) befindet sich in der Nähe der Belichtungstrommeloberfläche, berührt diese aber nie. Wenn er mit einer extrem hohen Spannung geladen wird, bildet sich ein elektrisches Feld (eine Korona), wodurch Entladungen stattfinden und die lichtempfindlichen Teilchen an der Trommeloberfläche aufgeladen werden. Eine Steuerungselektronik regelt dabei die Spannung und sorgt dafür, dass die Oberfläche der Trommel einer einheitlichen negativen Spannung zwischen ca. 600 und 1.000 Volt ausgesetzt wird.

Laser Der *Laser* fungiert als Schreibmechanismus des Druckers. Alle vom Laserstrahl belichteten Partikel auf der Trommel werden leitend, wodurch ihre Ladung zum geerdeten Kern der Trommel hin abfließt. Die gesamte Oberfläche der Trommel hat infolge der Aufladung durch den Koronadraht eine einheitliche negative Ladung zwischen ca. 600 und 1.000 Volt. Wenn Teilchen vom Laser getroffen werden, erfolgt eine Entladung und sie besitzen dann anschließend eine negative Ladung von ca. 100 Volt. Mit dem Laser lassen sich Bilder auf die Trommel »schreiben«. Beachten Sie, dass der Laser ein Positivbild auf die Trommel schreibt.

Toner Beim *Toner* im Laserdrucker handelt es sich um ein feines Pulver, das aus an Eisenpartikel gebundenen Kunststoffteilchen besteht. Die *Tonertrommel* sorgt für eine negative Ladung des Toners, die zwischen ca. 200 und 500 Volt beträgt. Da diese Ladung zwischen der ursprünglich einheitlichen negativen Ladung der lichtempfindlichen Trommel (600 bis 1.000 Volt) und der Ladung der vom Laser getroffenen Partikel auf der Trommeloberfläche (100 Volt) liegt, werden Tonerpartikel von jenen Bereichen der Belichtungstrommel angezogen, die vom Laser getroffen wurden (und die *relativ* zu den Tonerpartikeln positiv geladen sind).

Wichtig

Bei dem in Laserdruckern verwendeten schwarzen Toner handelt es sich üblicherweise um ein Gemisch aus Kohlenstoff-Schmelzen und Polyesterharz. Bei farbigem Toner werden statt des Kohlenstoffs andere Farbpigmente verwendet.

Unterer Koronadraht/Ladewalze Um das Bild von der Belichtungstrommel auf das Papier übertragen zu können, muss das Papier so geladen werden, dass die Tonerpartikel von der Trommel weg und auf das Papier gezogen werden. In älteren Druckern erledigt das der *untere Koronadraht* , ein dünner Draht, der von anderen dünnen Drähten geschützt wird und der das Papier positiv auflädt, wodurch negativ geladene Tonerpartikel auf das Papier gezogen werden. In neueren Geräten wird zu diesem Zweck eine sogenannte *Ladewalze* verwendet. Das positiv geladene Papier wird gleichfalls von der negativ geladenen Trommel angezogen. Damit sich das Papier nicht um die Trommel wickelt, wird seine statische Ladung durch den sogenannten *Entelektrisator* entfernt.

In den meisten Laserdruckern und gerade in großen, für den Einsatz in Unternehmen konzipierten Geräten befindet sich der untere Koronadraht bzw. die Ladewalze außerhalb der Tonerkartusche. Der untere Koronadraht ist eine besonders kritische Komponente, da er durch Toner und durch elektrostatische Anziehung leicht verschmutzt und daher gereinigt werden muss. Er kann aber auch leicht beschädigt werden, da er üblicherweise dünner als ein menschliches Haar ist. Den meisten Druckern mit freiliegendem unteren Koronadraht liegt zwar ein spezielles Werkzeug zur Reinigung bei, Sie können aber auch – äußerst vorsichtig – ein Wattestäbchen verwenden, das Sie in denaturierten Alkohol eintauchen. (Verwenden Sie keinen Reinigungsalkohol/Isopropylalkohol, da dieser Weichmacher enthält.) Generell sollten Sie keine Wartungsarbeiten an Druckern ausführen, ohne diese zuvor abgeschaltet und von der Stromversorgung getrennt zu haben.

Fixiereinheit Die *Fixiereinheit* (Fuser) ist fast immer von der Tonerkartusche getrennt. Sie lässt sich üblicherweise recht leicht ausfindig machen, da sie sich in der Nähe der Unterseite der Tonerkartusche befindet und in der Regel aus zwei Rollen zur Fixierung des Toners besteht. Manchmal ist die Fixiereinheit relativ gut in einem Gehäuse verborgen und schlecht zu erkennen, weil die Rollen dann nicht direkt sichtbar sind. Um die Position der Fixiereinheit zu ermitteln, denken Sie an den Papierweg im Drucker und daran, dass es sich beim Fixieren um den letzten Schritt des Druckprozesses handelt.

Der Toner liegt nach der Beseitigung der statischen Ladung des Papiers eigentlich nur noch locker auf der Oberfläche des Papiers. Der Toner muss permanent mit dem Papier verbunden werden, damit das Bild dauerhaft auf dem Papier bleibt. Zwei Rollen, eine Andruck- und eine Heizrolle, verschmelzen den Toner mit dem Papier. Die Andruckrolle wird gegen die Papierunterseite gedrückt, während die Heizrolle gegen die Oberseite drückt und den Toner mit dem Papier verschmilzt. Die Heizrolle ist mit einem nicht haftenden Material (z.B. Teflon) beschichtet, damit der Toner nicht an ihr haften bleibt.

Netzteile Alle in diesem Kapitel beschriebenen Geräte enthalten Netzteile, bei Laserdruckern sollten Techniker allerdings besondere Vorsicht walten lassen. Das *Hochspannungsnetzteil* versorgt den Koronadraht bzw. die Ladewalze mit einer extrem hohen Spannung, durch die das Hochspannungsnetzteil eines Laserdruckers zu einer der gefährlichsten Komponenten im PC-Bereich wird! Sie sollten Laserdrucker immer abschalten und vom Stromnetz trennen, bevor Sie deren Gehäuse öffnen, um Wartungsarbeiten vorzunehmen.

Antriebszahnräder Laserdrucker müssen viele mechanische Funktionen ausführen. Zunächst muss das Papier mithilfe einer Trennvorrichtung eingezogen, bedruckt und aus dem Drucker ausgeworfen werden. Dann muss die Belichtungstrommel gedreht und der Laser (oder ein Spiegel) von links nach rechts bewegt werden. Danach muss der Toner gleichmäßig verteilt und von der Fixiereinheit mit dem Papier verschmolzen werden. Schließlich muss das bedruckte Papier ausgeworfen und der Transportmechanismus gereinigt werden, damit das nächste Blatt bedruckt werden kann.

Besser ausgerüstete Drucker erlauben außerdem beidseitigen Druck und besitzen eine Duplex-Einheit, die einen Mechanismus zum Wenden des Papierblatts umfasst.

Wichtig

Die folgenden Komponenten eines Laserdruckers sollten Sie kennen: Belichtungstrommel, Fixiereinheit, Transportwalzen, Trennvorrichtung und Duplex-Einheit.

All diese Funktionen werden von komplexen, aus Zahnrädern bestehenden Antriebssystemen übernommen. In den meisten Laserdruckern werden diese Antriebssysteme zu Einheiten zusammengefasst, die im Allgemeinen *Getriebegehäuse* oder *Antriebseinheit* genannt werden. Die meisten Laserdrucker enthalten zwei oder drei Getriebegehäuse, die gegebenenfalls im Falle ihres seltenen Ausfalls relativ leicht ausgetauscht werden können. Die meisten Getriebegehäuse verfügen auch über eigene Motoren oder Magnetspulen für den Antrieb der Zahnräder.

Diese mechanischen Bauteile können verschleißen oder kaputtgehen und müssen gewartet bzw. ersetzt werden. Mehr dazu im Abschnitt über Fehlerbehebung später in diesem Kapitel.

Systemplatine Alle Laserdrucker enthalten wenigstens eine Platine mit elektronischen Bauteilen. Auf dieser Platine befinden sich der Hauptprozessor des Druckers, das Drucker-ROM und der Arbeitsspeicher zur Ablage des Bildes vor dem Drucken. Bei vielen Druckern befinden sich diese Funktionen auf zwei oder drei Platinen, die sich verteilt im Druckergehäuse befinden (siehe Abbildung 26.10). Bei älteren Druckern kann es auch einen separaten ROM-Chip und/oder einen speziellen Steckplatz zur Installation spezieller ROM-Chips geben, die üblicherweise der Nachrüstung spezieller Funktionen wie PostScript dienen.

Bei einigen Druckermodellen können Sie den Inhalt dieser ROM-Chips (die Firmware) aktualisieren, indem Sie einen Prozess ausführen, der als *ROM-Flashing* bezeichnet wird. Flashing ist der Aktualisierung des System-BIOS ganz ähnlich, die Sie in Kapitel 5, *BIOS und CMOS*, kennengelernt haben. Eine Aktualisierung der Firmware kann helfen, Fehler zu korrigieren, neue Funktionen hinzuzufügen oder die Schriften im Drucker zu aktualisieren.

Besonders wichtig ist der Arbeitsspeicher des Druckers. Wenn der Drucker nicht über genügend RAM zur Speicherung des Bildes vor dem Ausdruck verfügt, dann kann es zum Speicherüberlauf kommen. Einige Drucker speichern auch andere Daten im RAM, wie z.B. Schriftarten oder spezielle Befehle. Die Erweiterung des Arbeitsspeichers ist normalerweise ganz einfach, da man dazu nur ein oder zwei SIMM- oder DIMM-Bausteine in die entsprechenden Steckplätze einsetzen muss. Die Verwendung der *richtigen* RAM-Bausteine ist aber wichtig. Informieren Sie sich beim Druckerhersteller, welcher RAM-Typ verwendet werden muss. Auch wenn Ihnen die Hersteller gerne eigene, teure RAM-Module verkaufen, lassen sich bei den meisten Druckern herkömmliche DRAM-Bausteine einsetzen, die auch für Computer verwendet werden.

Ozonfilter Die Koronadrähte im Innern des Laserdruckers produzieren Ozon (O_3). In kleinen Dosen ist Ozon für Menschen ungefährlich, ist aber dennoch giftig und kann in höheren Konzentrationen z.B. Kopfschmerzen verursachen. Aber bereits in kleineren Konzentrationen kann es Druckerkomponenten beschädigen. Um diesem Problem zu begegnen, verfügen die meisten Laserdrucker über spezielle Ozonfilter, die in regelmäßigen Abständen mit einem Staubsauger gereinigt oder ersetzt werden müssen.

Sensoren und Schalter Alle Laserdrucker besitzen verschiedene Sensoren und Schalter, die über das ganze Gerät verteilt sind. Die Sensoren erkennen eine Vielzahl von Betriebszuständen, wie z.B. Papierstaus, eine leere Papierzufuhr oder Tonermangel. Viele dieser Sensoren sind eigentlich winzige Schalter, die offene Abdeckungen usw. erkennen. Meist arbeiten diese Sensoren/Schalter zuverlässig. Gelegentlich können sie aber auch verschmutzt oder beschädigt sein und dadurch dem Drucker falsche Signale senden. Meist genügt es, wenn man kontrolliert, ob es sich um ein echtes Problem oder die Falschmeldung eines Sensors/Schalters handelt.

3-D-Drucker

3-D-Drucker (Abbildung 26.12) verwenden geschmolzene Materialien, um dreidimensionale Objekte auszudrucken. Die meisten 3-D-Drucker verwenden zu diesem Zweck auf Rollen befindliche Kunststoff-Filamente (Abbildung 26.13). Manche 3-D-Drucker können für den Ausdruck verschiedene Farben verwenden.

3-D-Drucker bauen das Objekt anhand der 3-D-Daten Schicht für Schicht der Reihe nach scheibchenweise auf. Einfache 3-D-Drucker können weniger komplexe Formen wie Blöcke, Pyramiden, Zylinder und dergleichen ausgeben. Bessere Modelle können auch interessantere Strukturen ausdrucken, wie

beispielsweise die Spielfiguren für das beliebte Brettspiel *Die Siedler von Catan* (Abbildung 26.14). Noch bessere Modelle können noch komplexere Formen ausdrucken, die Hohlräume und Lücken in den Schichten enthalten.

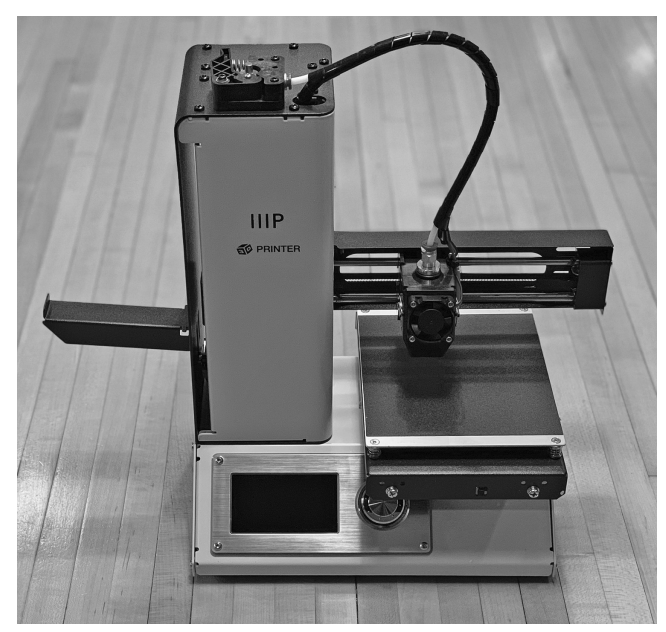


Abb. 26.12: 3-D-Drucker



Abb. 26.13: Kunststoff-Filamente für den 3-D-Druck



Abb. 26.14: Mit dem 3-D-Drucker hergestellte Spielfiguren (Foto mit freundlicher Genehmigung von Donny Jansen)

Die Einrichtung eines 3-D-Druckers ist nicht so einfach wie die Installation eines normalen Druckers. Der Anschluss erfolgt zwar normalerweise über USB und auch die Treiber sind typisch, aber 3-D-Drucker müssen auch die Zufuhr der Kunststoff-Filamente steuern können. Darüber hinaus benötigt man spezielle Software, die für den 3-D-Druck ausgelegt ist. Die 3-D-Drucksoftware der meisten Hersteller kann Standardformate für 3-D-Zeichnungen wie STL-, OBJ- oder CAD-Dateien verwenden. Abbildung 26.15 zeigt die Software Ultimaker Cura bei der Ausgabe eines Druckauftrags auf einem 3-D-Drucker.

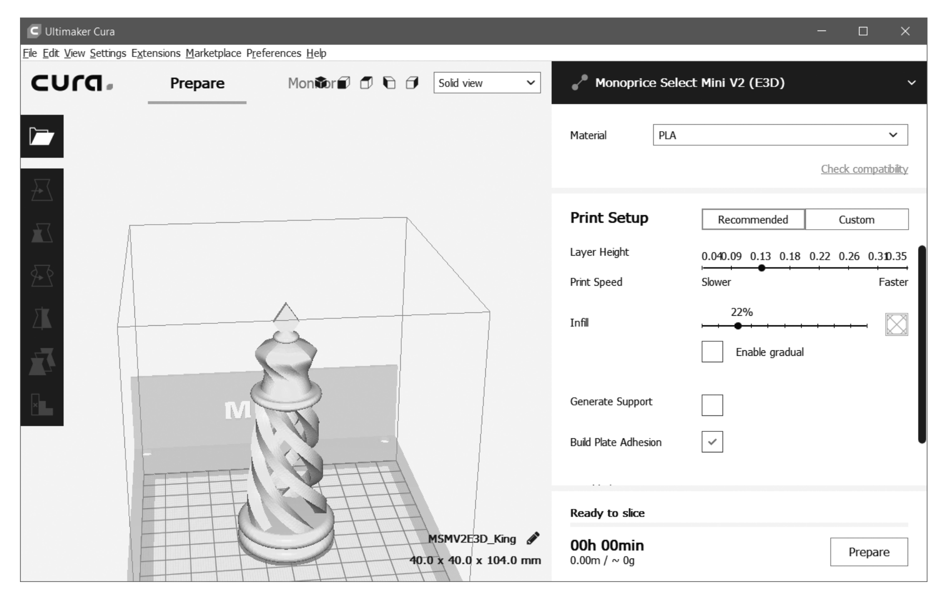


Abb. 26.15: Ausgabe eines 3-D-Druckauftrags

Virtuelle Drucker

Der eigentümlichste Drucker dürfte der *virtuelle Drucker* sein. Man sieht es ihm zwar nicht an, aber tatsächlich hat die Ausgabe auf einem virtuellen Drucker große Ähnlichkeit mit »richtigem« Drucken. Wenn Sie etwas auf einem virtuellen Drucker ausgeben, durchläuft Ihr System bei den Druckvorbereitungen dieselben Schritte wie beim richtigen Drucken, nur wird das Ergebnis nicht an einen Drucker gesendet, sondern einem Programm übergeben, das die Ausgabe Ihres Computers in eine Datei schreibt. Der Inhalt dieser Datei entspricht dem, was Sie auf der ausgedruckten Seite sehen würden. Sie können diese Datei später bei Bedarf ausdrucken oder sie jemand anderem zum Ausdrucken übersenden, Sie können sie aber auch im digitalen Format belassen. Virtuelle Drucker stellen eine praktische Möglichkeit bereit, alles Ausdruckbare als Datei zu speichern, und sind besonders gut dazu geeignet, Kopien von im Internet gefundenen Informationen zu erstellen. Die CompTIA ist der Ansicht, dass Sie einige der verfügbaren Optionen kennen sollten, sehen wir sie uns also an!

Wichtig

Die Lernziele der CompTIA A+-Zertifizierungsprüfung erwähnen die Druckoption AUSGABE IN DATEI UMLEITEN, die eine Datei speichert, die später ausgedruckt werden kann, ohne das Programm zu verwenden, das sie erzeugt hat. Allerdings handelt es sich hierbei um eine veraltete Option, die oft im Dialogfeld DRUCKEN als Kontrollkästchen auftaucht, aber zumeist nicht richtig funktioniert, wenn Sie einen USB-Drucker benutzen. Selbst wenn es funktioniert, kann die Datei Probleme bereiten. Sie sollten diese Option zwar kennen, aber besser eine der hier beschriebenen Methoden verwenden.

Ausgabe als PDF Eine der beliebtesten Optionen ist die Ausgabe als PDF, eine Funktion, die viele Betriebssysteme heutzutage von Haus aus unterstützen. Windows kann das allerdings erst ab Version 10. Unter älteren Windows-Versionen müssen Sie also einen virtuellen PDF-Drucker installieren. Sie können die offizielle Software von Adobe verwenden, es gibt aber auch Lösungen von Drittanbietern.

Ausgabe als XPS Im nächsten Abschnitt nehme ich XPS genauer unter die Lupe, aber seit Vista enthält Windows den *Microsoft XPS Document Writer* als Drucker, mit dem Sie `.xps`-Dateien ausgeben können, die sich mit dem zum Betriebssystem dazugehörigen XPS-Viewer anzeigen lassen. Die Unterstützung für `.xps`-Dateien in anderen Betriebssystemen ist durchwachsen, es gibt aber Software von Drittanbietern, die das Verwenden dieses Formats ermöglicht.

Ausgabe als Bild Mit dieser Option können Sie eine ganz normale Bilddatei speichern, wie z.B. BMP, GIF, JPG, PNG, TIFF oder andere. Bilddateien sind allerdings für viele Dokumente schlecht geeignet – Text wird nicht skaliert und kann nicht durchsucht, ausgewählt oder kopiert werden. Andererseits lassen sich Bilddateien auf praktisch allen Betriebssystemen und Geräten anzeigen. Um die Druckausgabe als Bilddatei in einem bestimmten Format zu speichern, benötigen Sie im Allgemeinen Software eines Drittanbieters.

Ausgabe über die Cloud Die scharfe Grenze zwischen herkömmlichen und virtuellen Druckern löst sich auf, wenn man Anwendungen wie *Google Cloud Print* betrachtet, die einen virtuellen Drucker auf Ihrem System installieren, der die virtuell gedruckten Dokumente auf einem Cloud-Server ablegt, der dafür sorgt, dass sie schließlich auf einem echten Drucker ausgegeben werden – und all das, ohne einen Druckertreiber installieren zu müssen.

Druckersprachen

Da Sie nun die verschiedenen Druckertypen und Drucktechnologien kennen, stellt sich die Frage, wie Drucker mit dem PC kommunizieren. Wie lässt sich dem Drucker mitteilen, dass er den Buchstaben »A« oder das Bild eines Leguans ausgeben soll? Drucker verstehen vordefinierte Druckersprachen, mit denen sich sowohl Zeichen als auch Grafiken verarbeiten lassen. Die Software muss bei der Kommunikation mit dem Drucker die richtige Sprache sprechen, damit der Drucker die Dokumente korrekt zu Papier bringt. Sehen wir uns einmal einige verbreitete Druckersprachen an.

ASCII Üblicherweise denkt man bei »ASCII« nur an einen standardisierten Zeichensatz, der aus dem Basisalphabet mit seinen Klein- und Großbuchstaben und einigen fremdartigen Symbolen besteht. *ASCII* enthält aber eine ganze Reihe von Steuercodes für die Übertragung von Daten, die teilweise zur Steuerung von Druckern eingesetzt werden können. Der ASCII-Code 10 (hexadezimal: 0Ah) bedeutet z.B. Zeilenvorschub (LF – Line Feed), der ASCII-Code 12 (0Ch) Seitenvorschub (FF – Form Feed). Diese Befehle waren bereits standardisiert, bevor es den IBM-PC überhaupt gab, und werden von allen Druckern verstanden. Wenn das nicht der Fall wäre, würde die Taste DRUCK nicht bei allen Druckern funktionieren. Die hohe Standardisierung hat ihre Vorteile, auch wenn die Möglichkeiten mit diesen Steuercodes äußerst beschränkt sind. Wenn man qualitativ hochwertige Grafiken oder eine Vielzahl verschiedener Schriftarten drucken will, braucht man leistungsfähigere Druckersprachen.

PostScript Adobe Systems hat die Seitenbeschreibungssprache *PostScript* in den frühen 1980ern als eine geräteunabhängige Druckersprache entwickelt, die hochauflösende Grafik und skalierbare Schriftarten bewältigt. PostScript-Interpreter lassen sich in Druckgeräte integrieren. Da PostScript von den Druckern auf der Hardwareebene verstanden wird, übernimmt der Drucker, und nicht der Systemprozessor des Rechners den größten Teil der Bildverarbeitung, daher sind PostScript-Drucker schneller. PostScript baut eine Seite als einziges großes Rasterbild auf, daher lassen sich PostScript-Dateien besonders gut von einer Rechnerplattform auf eine andere übertragen. Die Dateien lassen sich auf einem Rechner oder einer Betriebssystemplattform erstellen und problemlos auf einem anderen Rechner oder einer anderen Plattform (wie z.B. auf hochwertigen Satzmaschinen) ausgeben.

PCL (Printer Command Language) *PCL* ist eine von Hewlett-Packard entwickelte erweiterte Druckersprache mit einem umfangreichen Druckerbefehlssatz, der weit über die Möglichkeiten von ASCII hinausgeht. PCL wurde von Hewlett-Packard vorrangig für die Ausgabe von Texten konzipiert. Es unterstützt keine anspruchsvollen grafischen Funktionen. Die jüngste Version von PCL (PCL6) bietet zwar skalierbare Schriftarten und zusätzliche Funktionen zum Zeichnen von Linien, ist aber im Unterschied zu PostScript von der Druckerhardware abhängig. PCL ist keine echte Seitenbeschreibungssprache, da die Zeichen auf dem Papier nicht über eine Reihe von Befehlen definiert werden. Die Befehle müssen von dem jeweiligen Druckermodell unterstützt werden, weshalb PCL-Dateien weniger portabel als PostScript-Dateien sind.

Wichtig

In der Liste der Akronyme der CompTIA ist PCL als *Printer Control Language* aufgeführt. Ob Command oder Control, spielt heute eigentliche keine Rolle mehr. HP benutzt in der Dokumentation immer nur die Abkürzung PCL.

Windows GDI und XPS Unter Windows ist die *GDI*-Komponente (*Graphical Device Interface* – grafische Geräteschnittstelle) des Betriebssystems für Druckfunktionen zuständig. Auch wenn man externe Druckersprachen (z.B. PostScript) benutzen *kann*, installieren die meisten Anwender ihre Drucker einfach nur und überlassen Windows die ganze weitere Arbeit. Die GDI nutzt den Prozessor des Rechners und nicht den des Druckers zur Verarbeitung eines Druckauftrags und überträgt dann den fertiggestellten Auftrag zum Drucker. Wenn Sie z.B. unter Windows einen Buchstaben in einer TrueType-Schriftart drucken, verarbeitet die GDI den Druckauftrag und überträgt dann ein Rasterbild (Bitmap) der jeweiligen Seite zum Drucker. Für den Drucker ist eine Seite mit TrueType-Text daher ein Bild und kein Text. Solange der Drucker leistungsfähig genug und mit genügend Speicher ausgestattet ist, müssen Sie sich keine weiteren Gedanken über die vom Drucker verwendete Sprache machen. Mit dem Drucken unter Windows werde ich mich später in diesem Kapitel noch eingehender befassen.

Mit Windows Vista wurde darüber hinaus aber noch ein weiteres Druckverfahren eingeführt, das sogenannte *XPS* (*XML Paper Specification*) XPS bietet verglichen mit GDI einige Verbesserungen, zu denen ein besseres Farbmanagement (das mit dem Windows-Farbsystem zusammenarbeitet) und erweiterte Layoutmöglichkeiten gehören. Für den XPS-Druck wird ein Treiber benötigt, der XPS unterstützt. Einige Drucker unterstützen XPS aber auch direkt, sodass die Ausgabedaten vor dem Drucken nicht erst noch in eine gerätespezifische Druckersprache umgewandelt werden müssen.

26.1.2 Scanner

Mit einem Scanner können Sie digitale Kopien von Fotos, Dokumenten, Zeichnungen usw. erstellen. Mit besseren Scannern können Sie oft auch Dias oder Negative direkt kopieren, was zu Bildern erstaunlicher Qualität führt, sofern das Originalfoto nur halbwegs gut ist! In diesem Abschnitt sehen wir uns an, wie Scanner funktionieren, und dann erkläre ich, wie Sie den richtigen Scanner für sich selbst oder Ihre Kunden auswählen können.

Funktionsweise von Scannern

Die sogenannten *Flachbettscanner* sind die gebräuchlichste Variante von Scannern und sie funktionieren alle auf die gleiche Weise. Sie legen ein Foto oder eine andere Vorlage auf das Glas, schließen den Deckel und starten das Scannen mit irgendeiner Software. Der Scanner führt ein helles Licht einmal oder mehrmals am Glas entlang, um das Bild aufzunehmen. Abbildung 26.16 zeigt einen geöffneten Scanner.



Abb. 26.16: Offener Scanner mit aufgelegtem Foto

Hinweis

Viele bessere Scanner oder Multifunktionsgeräte besitzen einen automatischen Papiereinzug, in den man mehrere Dokumente einlegen kann, die das Gerät dann der Reihe nach einzieht. Auf diese Weise kann das Scannen mehrerer Seiten automatisiert werden.

Die Scan-Software, mit der die Hardware gesteuert wird, kann ganz unterschiedlich aussehen. Die meisten Hersteller benutzen eigene Treiber und weitere Programme, um eine Schnittstelle zwischen Rechner und Scanner herzustellen. Wenn Sie beispielsweise am Epson Perfection die Taste auf der Vorderseite drücken, öffnet sich die Epson-Software und ist bereit zum Scannen (Abbildung 26.17).

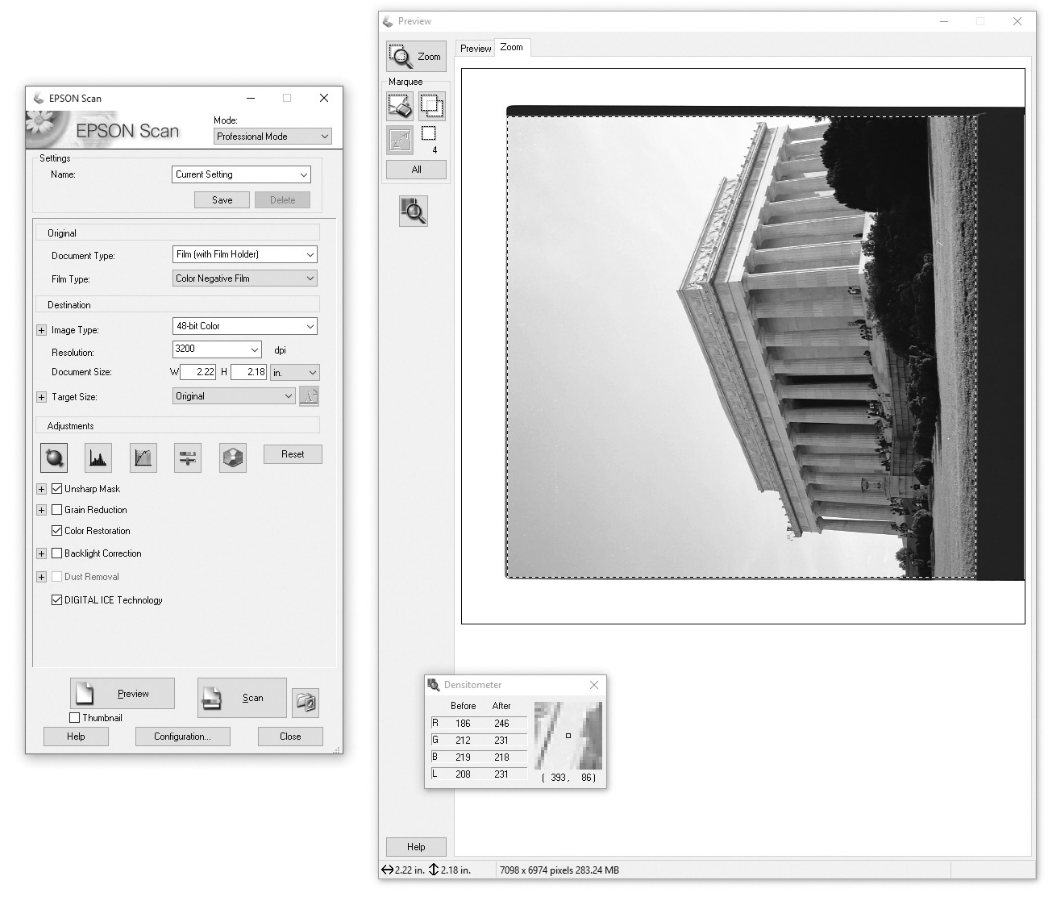


Abb. 26.17: Epson-Software zum Scannen

Sie können auch zuerst Ihre bevorzugte Bildbearbeitungssoftware starten und dann ein Bild von einem Scanner importieren. Abbildung 26.18 zeigt die Funktion zum Importieren eines Bildes vom Scanner in dem verbreiteten und kostenlosen Bildbearbeitungsprogramm *GIMP* (GNU Image Manipulation Program). Wie in vergleichbaren Programmen wählen Sie hier erst DATEI|IMPORTIEREN und dann eine Quelle. Im Beispiel wird der traditionelle *TWAIN*-Treiber genutzt. TWAIN steht übrigens für *Technology Without an Interesting Name* (das habe ich mir nicht ausgedacht!) und ist seit Langem der Standardtreibertyp für Scanner.

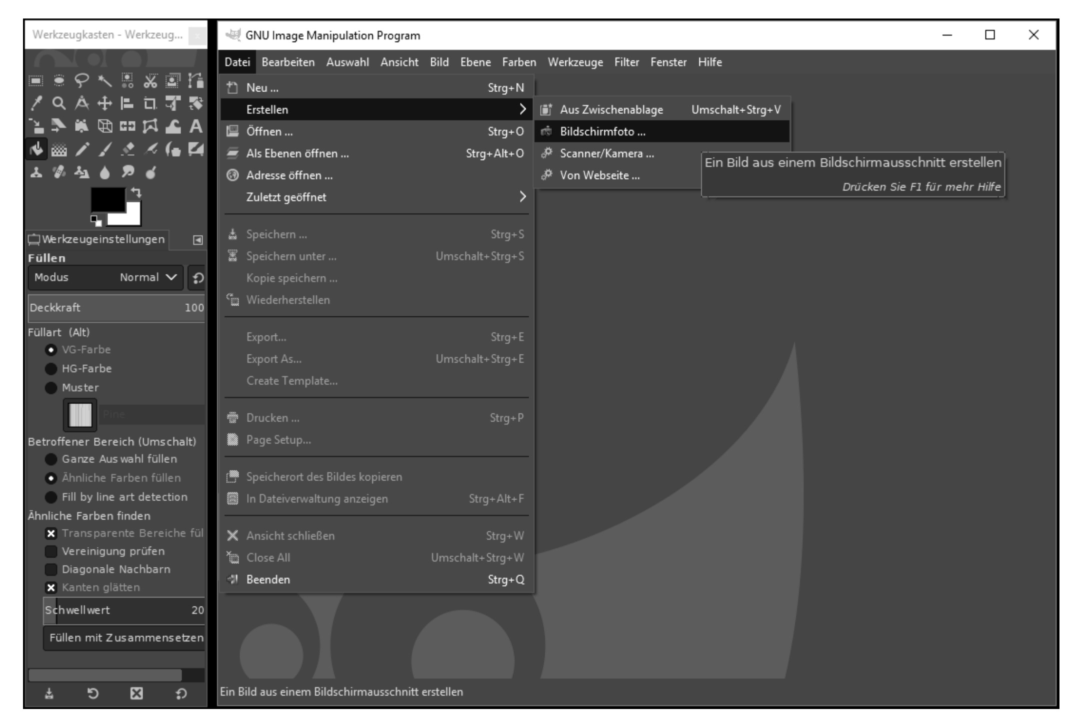


Abb. 26.18: Ein Bild vom Scanner in GIMP importieren

Jetzt kommen die Treiber und anderen Programme, die den Scanner steuern, ins Spiel, und stellen (wie in Abbildung 26.17) eine Benutzeroberfläche für den Scanner bereit. Hier können Sie meist die Auflösung und mehr oder weniger zahlreiche weitere Optionen einstellen.

Hinweis

Mit einem Scanner können Sie nicht nur Bilder einlesen. Viele Scanner bieten eine sogenannte optische Zeichenerkennung (*Optical Character Recognition*, OCR), die es ermöglicht, dass der Computer ein Bild einliest und in einen Text umwandelt, der mit einem Textverarbeitungsprogramm bearbeitet werden kann.

Die Auswahl eines Scanners

Bei der Auswahl eines Scanners sind vier Kriterien zu berücksichtigen: Auflösung, Farbtiefe, Graustufentiefe und Scan-Geschwindigkeit. Die drei ersten können Sie beim Scannen einstellen, aber nur auf Werte, die unter dem möglichen Maximum liegen. Die Scan-Geschwindigkeit hängt von den übrigen Parametern ab, und die maximale Geschwindigkeit wird von der Scanner-Hardware bestimmt.

Konfigurierbare Variablen Scanner wandeln das gescannte Bild in ein Punktraster um. Die maximale Anzahl an Punkten bestimmt, wie detailliert Bilder aufgenommen werden können und wie sie bei Vergrößerungen aussehen. Größtenteils wird der Begriff *Auflösung* zur Angabe der Feinheit des Rasters verwendet. Wie Sie sich wahrscheinlich vorstellen können, gilt: Je höher die Auflösung, desto detaillierter wird das eingescannte Bild und desto besser lässt es sich vergrößern.

Ältere Scanner erzeugen nur Bilder mit Maximalauflösungen von 600 x 600 dpi (Dots per Inch), während neuere Modelle üblicherweise die vierfache und professionelle Geräte sogar noch höhere Werte erreichen können. Die Hersteller geben oft zweierlei Werte für die Scannerauflösung an: die tatsächliche Auflösung der Scanneroptik (optische Auflösung) und die erweiterte oder interpolierte Auflösung, die ein Scanner mithilfe integrierter Software erreichen kann.

Angaben zur interpolierten Auflösung sagen im Prinzip nichts aus. Ich empfehle mindestens eine optische Auflösung von 2.400 x 2.400 dpi; wenn die Bilder aber nur im Internet veröffentlicht werden sollen, dann reicht auch eine niedrigere Auflösung aus.

Über die *Farbtiefe* wird festgelegt, wie viele Bits ein Scanner zur Beschreibung der Farbe eines einzelnen Punktes benutzt. Diese Zahl gibt die Farbe, den Farbton, die Sättigung usw. an. Höhere Werte stehen also für eine wesentlich bessere Bildqualität. Bei Binärzahlen sorgt jedes zusätzliche Bit für eine Verdopplung der Qualität. Die gängigsten Farbtiefen aktueller Scanner sind 24 und 48 Bit. Beispielsweise lassen sich mit einem 24-Bit-Scan jeweils 256 Farbvariationen je Subpixel (Rot, Grün, Blau) speichern. Das entspricht insgesamt 16.777.216 möglichen Farben im eingescannten Bild, daher ist in den Einstellungen oft von »Millionen Farben« die Rede. Bei einem 48-Bit-Scan sind es bereits 65.536 Farbvariationen pro Subpixel und der Scan kann satte 281.474.976.710.656 Farben enthalten. Nachteil dieser Farbvielfalt ist, dass 48-Bit-Scans doppelt so viel Speicher wie 24-Bit-Scans belegen und schnell mehrere Hundert Megabyte groß werden.

Heutzutage sind 48-Bit-Scanner derart verbreitet, dass Sie sich selbst bei knappem Budget nicht mit weniger zufriedengeben sollten. Abbildung 26.19 und die beiden darauf folgenden Abbildungen sollen Ihnen einen Eindruck von den unterschiedlichen Auflösungen beim Scannen vermitteln.



Abb. 26.19: Ohrring, gescannt mit 72 dpi und 24 Bit Farbtiefe



Abb. 26.20: Derselbe Ohrring, gescannt mit 300 dpi und 24 Bit Farbtiefe

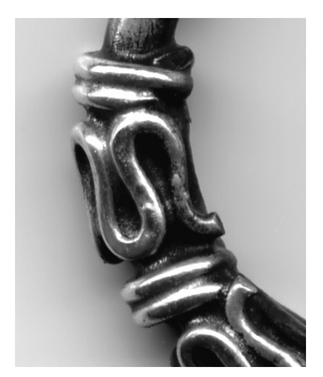


Abb. 26.21: Nochmals derselbe Ohrring, gescannt mit 1200 dpi und 24 Bit Farbtiefe

Scanner unterscheiden sich ganz wesentlich in der *Graustufentiefe*, einer Zahl, die definiert, wie viele Graustufen sie bei einzelnen Bildpunkten speichern können. Das spielt vor allem dann eine Rolle, wenn Sie mit Schwarz-Weiß-Bildern arbeiten, weil die Graustufentiefe normalerweise sehr viel kleiner als die Farbtiefe ist. Die aktuellen Scanner für Privatbenutzer unterstützen Graustufentiefen von 8, 12 und 16 Bit. Vergleichen Sie das mit den eben erwähnten Werten für die Farbtiefe, denn für Schwarz-Weiß-Bilder sind nur ein Drittel der Informationen erforderlich, die zum Speichern der Rot-, Grün- und Blau-Werte eines farbigen Bildes nötig sind. Ich empfehle 16 Bit.

Scan-Geschwindigkeit Scanner haben eine von ihrer Hardware bestimmte maximale Scan-Geschwindigkeit. Die Zeit für die Ausführung eines Scans wird auch durch die von Ihnen eingestellten Parameter bestimmt und verlängert sich, wenn Sie mehr Details aufnehmen wollen. Ein typischer, einfacher Scanner benötigt beispielsweise mehr als 30 Sekunden, um ein 10 x 15 cm großes Foto mit 300 dpi zu scannen. Ein schnellerer Scanner schafft dies hingegen innerhalb von zehn Sekunden.

Wenn Sie die Auflösung des Scans auf 600 dpi bei einer Farbtiefe von 48 Bit erhöhen, können auch schnellere Scanner eine Minute bis zum fertigen Bild benötigen. Verwenden Sie die für Ihre Bedürfnisse optimalen Einstellungen. Versuchen Sie nicht, immer den bestmöglichen Scan durchzuführen, wenn Sie die Auflösung und Farbtiefe gar nicht brauchen.

Tipps zum Scannen

Als allgemeine Regel sollten Sie den besten Scan erzeugen, den Sie verarbeiten können, und dann mit der Größe und Bildqualität herumexperimentieren, wenn Sie Scans ausdrucken oder im Web bereitstellen möchten. Die Größe des Arbeitsspeichers in Ihrem System und zum Teil auch die Prozessorgeschwindigkeit bestimmen, wie groß die von Ihnen verarbeiteten Dateien sein dürfen.

Wenn Sie viel unterwegs sind, sollten Sie die Transportsicherung der Scanner-Beleuchtung verriegeln. Entriegeln Sie ihn aber unbedingt wieder, bevor Sie den Scanner benutzen, sonst bleibt das Beleuchtungselement an seiner Position hängen. Damit machen Sie keine besonders guten Scans!

26.1.3 Kopieren und Faxen

Die Scan- und Druckfähigkeiten ermöglichen es den Herstellern, ihren Multifunktionsgeräten eine Kopierfunktion zu verleihen. Im Grunde genommen wird beim Kopieren eines Fotos oder Dokuments ein Scan durchgeführt, der dann ausgedruckt wird – aber eben mit nur einem Tastendruck.

Zum Faxen sind ein Papiereinzug sowie ein herkömmlicher analoger Telefonanschluss erforderlich. Das Faxen an sich ist ein Kinderspiel: Legen Sie das Dokument in den Papiereinzug, geben Sie die Faxnummer ein und drücken Sie auf die »Senden«-Taste.

26.1.4 Automatischer Papiereinzug

Multifunktionsgeräte verwenden beim Kopieren, Scannen oder Faxen einen automatischen Papiereinzug, der sich typischerweise auf der Oberseite des Geräts befindet. In dieses Fach werden die Papierseiten eingelegt (Abbildung 26.22). Die bedruckte Seite der Blätter muss in eine bestimmte Richtung weisen. Meistens gibt es eine Kennzeichnung, die angibt, wie die Seiten ausgerichtet werden müssen (Abbildung 26.23).



Abb. 26.22: Typischer automatischer Papiereinzug



Abb. 26.23: Die Kennzeichnung gibt an, wie die Seiten ausgerichtet werden müssen.

26.1.5 Anschlüsse

Die meisten Drucker, Scanner und Multifunktionsgeräte werden per USB angeschlossen, WLAN- und Ethernet-Verbindungen erfreuen sich aber auch großer Beliebtheit. Sie sollten sowohl die über das Netzwerk verbundenen Geräte als auch die per USB anschließbaren kennen.

USB-Verbindung

Aktuelle Drucker und Multifunktionsgeräte werden per USB-Anschluss mit dem Computer verbunden. Manchen Druckern liegt kein USB-Kabel bei, Sie müssen es in diesem Fall zusätzlich erwerben. (Es ist eine ziemliche Enttäuschung, wenn man zu Hause den neuen Drucker auspackt und feststellt, dass man ihn nicht anschließen kann, weil das Kabel fehlt.) Die meisten Drucker verwenden USB-Kabel mit einem Standard-USB-Typ-A-Stecker an einem Ende und einem Typ-B-Stecker am anderen, manche aber auch Typ-A-Stecker an beiden Enden. Welche Stecker zum Einsatz kommen, spielt letztlich aber keine Rolle. Schließen Sie einfach ein passendes USB-Kabel an!

Netzwerkverbindung

Dass Drucker oder Multifunktionsgeräte nur in Unternehmensumgebungen über das Netzwerk angeschlossen werden, ist schon länger nicht mehr der Fall. Auch immer mehr Privathaushalte erfreuen sich der Vorteile von Netzwerkdruckern. Früher war es üblich, den Drucker an einem einzelnen PC anzuschließen und dann eine Druckerfreigabe einzurichten, damit andere über das Netzwerk auf den Drucker zugreifen können. Diese Vorgehensweise hat allerdings den Nachteil, dass der mit dem Drucker verbundene Computer eingeschaltet sein muss, wenn jemand den Drucker verwenden möchte.

Heutzutage sind typische Netzwerkdrucker mit einem WLAN-Adapter ausgestattet (nach 802.11 a, b, g, n oder ac), der es ermöglicht, über eine Infrastruktur- oder eine Ad-hoc-Verbindung drahtlos zu drucken. Auf Ad-hoc-Verbindungen sollten Sie allerdings aus Sicherheitsgründen möglichst verzichten. Wie ein drahtloses Ad-hoc-Netzwerk eingerichtet wird, können Sie in Kapitel 20, *Drahtlose Netzwerke*, nachlesen.

In anderen Netzwerkdruckern ist ein Netzwerkadapter mit Standard-Ethernet-Anschluss (RJ-45-Buchse) eingebaut, über den das Gerät direkt oder mit dem Router verbunden wird. Dem Drucker wird üblicherweise eine statische IP-Adresse zugewiesen, oder er erhält sie von einem DHCP-Server. (Wenn Ihnen die Begriffe Router, IP-Adresse oder DHCP-Server nichts sagen, können Sie in den Kapiteln 18 und 19 nachschlagen.) Wenn der Drucker erst einmal mit dem Netzwerk verbunden ist, arbeitet er unabhängig von einem Computer. Manche Drucker werden auch über eine Bluetooth-Schnittstelle angesprochen.

Hinweis

Da die Lebensdauer von Druckern tendenziell diejenige der meisten anderen Geräte übertrifft, müssen Sie damit rechnen, dass drahtlos nutzbare Drucker einen der älteren WLAN- oder Bluetooth-Standards verwenden.

Wenn ein Drucker keine eingebaute Ethernet-, WLAN- oder Bluetooth-Schnittstelle besitzt, können Sie sich ein eigenständiges netzwerkfähiges Gerät beschaffen, das als *Druckerserver* bezeichnet wird, um Ihren Drucker mit dem Netzwerk zu verbinden. Sie sollten allerdings wissen, dass Sie vermutlich nicht alle Funktionen eines an einem Druckerserver angeschlossenen Multifunktionsgeräts nutzen werden können. Druckerserver, die eine Ethernet- oder WLAN-Schnittstelle besitzen, ermöglichen es, einen oder mehrere Drucker per USB (oder via Parallelanschluss, falls Ihr Drucker so alt ist) anzuschließen. Vielleicht haben Sie sogar schon einen Druckerserver. Überprüfen Sie, ob Ihr Router über einen integrierten Druckerserver verfügt. Ist das der Fall, können Sie Ihren Drucker womöglich am USB-Port des Routers anschließen. Nehmen Sie den uralten Matrixdrucker und binden Sie ihn ins Netzwerk ein – worauf warten Sie noch?

Wichtig

Ein Druckerserver muss kein eigenständiges Gerät sein. Auch Ihr Windows-System kann als Druckerserver fungieren. Wenn Sie für einen an Ihrem Computer angeschlossenen Drucker eine Druckerfreigabe einrichten, arbeitet Ihr System als Druckerserver.

Weitere Verbindungen

Zum Anschließen von Druckern sind viele weitere Verbindungstypen verfügbar. Ich habe mich hier auf USB- und Netzwerkverbindungen konzentriert, Sie könnten in der Praxis aber auch alten Druckern begegnen, die einen Parallelanschluss, einen seriellen Anschluss oder SCSI verwenden. Das ist zwar nicht wahrscheinlich, aber durchaus möglich. Vielleicht läuft Ihnen auch ein eigenständiger Scanner mit Thunderbolt-Anschluss über den Weg.

26.2 Funktionsweise des Laserdruckers

Der Druckprozess kann beim Laserdrucker in sieben Schritte unterteilt werden, die Sie für die CompTIA A+-Prüfung kennen sollten. Als Techniker sollten Sie mit diesen Phasen vertraut sein, weil Ihnen das hilft, Druckprobleme zu lösen. Wenn beispielsweise in der Mitte einer Seite eine seltsame Linie gedruckt wird, wissen Sie, dass es ein Problem mit der Belichtungstrommel oder dem Reinigungsmechanismus gibt und die Tonerkartusche gewechselt werden muss.

Bei den meisten Laserdruckern besteht der Druckprozess aus sieben Schritten. Merken Sie sich aber, dass einige Laserdrucker möglicherweise ein wenig von der beschriebenen Vorgehensweise abweichen, auch wenn der Prozess meist in dieser Reihenfolge abläuft:

1. Verarbeiten
2. Laden
3. Belichten
4. Entwickeln
5. Übertragen
6. Fixieren
7. Reinigen

26.2.1 Verarbeiten

Wenn Sie in einem Programm auf DRUCKEN klicken, geschehen verschiedene Dinge. Die CPU verarbeitet Ihren Druckauftrag und stellt ihn in die Druckerwarteschlange, die es ermöglicht, mehrere Druckaufträge zu erteilen, die der Drucker dann der Reihe nach abarbeitet. Nun sendet Windows den ersten Druckauftrag an den Drucker. Hier gibt es potenziell den ersten Engpass. Handelt es sich um

einen großen Druckauftrag, kann das Betriebssystem ihn nur häppchenweise an den Drucker übergeben und im Infobereich unten rechts auf dem Bildschirm wird ein Druckersymbol angezeigt. Verschwindet das Symbol wieder, ist die Druckerwarteschlange leer und alle Aufträge wurden an den Drucker übermittelt.

Sobald die Übergabe des Druckauftrags erfolgt ist, übernimmt die Druckerhardware und beginnt mit der Verarbeitung. Dies ist der zweite potenzielle Engpass, der sich aus mehreren Komponenten zusammensetzt.

Rasterbilder

Bei Anschlagdruckern werden die Daten zeichen- oder zeilenweise übertragen, während bei Laserdruckern jeweils komplette Seiten übermittelt werden. Laserdrucker erzeugen ein *Rasterbild* (eine Ansammlung von Bildpunkten) der Seite, das dem Endergebnis entspricht. Der Drucker benutzt den Laser, um das Rasterbild auf die Belichtungstrommel zu »zeichnen«. Da der Laserdrucker die gesamte Oberfläche der Trommel belichten muss, bevor die Übertragung des Bildes auf das Papier stattfinden kann, wird stets eine komplette Seite verarbeitet.

Laserdrucker verfügen mit dem sogenannten *RIP* (*Raster Image Processor*) über einen Chip, der das an den Drucker übertragene Rasterbild in Befehle für den Laser übersetzt. Tintenstrahldrucker verwenden ebenfalls RIPs, aber diese sind Teil des Gerätetreibers und die Verarbeitung findet nicht auf dem Drucker statt. Der RIP benötigt RAM, um die zu verarbeitenden Daten zwischenspeichern zu können.

Laserdrucker benötigen also ausreichend Arbeitsspeicher für eine komplette Seite. Einige hochauflösende Bilder erfordern möglicherweise so viel Speicher, dass es zu einem Speicherüberlauf (Memory Overflow) kommt. Wenn ein Speicherüberlauf gemeldet wird, dann können Sie versuchen, die Seite in verringerter Auflösung, mit verkleinerten Abbildungen oder abgeschaltetem RET (über diese Option erfahren Sie mehr im nachfolgenden Abschnitt) zu drucken. Die einfachste und wirksamste Methode, um dem Speicherüberlauf zu begegnen, ist aber natürlich die Erweiterung des Arbeitsspeichers des Laserdruckers.

Glauben Sie aber nicht, dass sich alle Fehler im Zusammenhang mit dem Speicher durch die einfache Erweiterung des Druckerspeichers beheben lassen. Genau wie das Hinzufügen weiterer RAM-Chips nicht alle Probleme des herkömmlichen PC-Speichers beheben kann, kann auch eine Erweiterung des Arbeitsspeichers bei Laserdruckern nicht alle Speicherprobleme beseitigen. Bei einem HP LaserJet bedeutet die Fehlermeldung »21 Error« zum Beispiel, dass der Drucker »sehr komplexe Daten nicht schnell genug für den Druck aufbereiten kann«. Das heißt nichts weiter, als dass die Daten einfach zu komplex für den RIP sind. Eine Speichererweiterung würde diese Fehlermeldung *nicht* beseitigen und wäre Geldverschwendung. Es bleibt Ihnen hier nichts anderes übrig, als die Druckseite weniger komplex zu gestalten.

Auflösung

Ähnlich wie Bildschirme unterschiedliche Auflösungen beherrschen, können Laserdrucker in verschiedenen Auflösungen drucken. Die maximale Auflösung eines Laserdruckers wird von seinen physischen Merkmalen bestimmt. Die Auflösung von Laserdruckern wird in dpi (dots per inch – Druckpunkte je Zoll) angegeben. Übliche Auflösungen sind 2.400 x 600 oder 1.200 x 1.200 dpi. Die erste Zahl gibt die horizontale Auflösung an und wird davon bestimmt, wie fein der Laser fokussiert werden kann. Die zweite Zahl wird von der kleinsten Größeneinheit bestimmt, mit der die Trommel gedreht werden kann. Höhere Auflösungen führen zu einer besseren Ausgabequalität. Sie sollten aber berücksichtigen, dass sie auch mehr Speicher erfordern. In einigen Fällen lassen sich komplexe Bilder wegen ihres großen Speicherbedarfs nur in niedrigeren Auflösungen drucken. Selbst bei 300-dpi-Ausdrucken können Laserdrucker durch Einsatz von *RET*-Technologien (*Resolution Enhancement Technology*) qualitativ weit bessere Ausdrucke als Matrixdrucker erzeugen.

Beim Einsatz von RET werden kleinere Punkte bzw. Punkte in abgestuften Größen gedruckt, wodurch sich die treppenförmigen Kanten zwischen benachbarten Druckpunkten glätten lassen, die für Drucker ohne *Kantenglättungsverfahren* typisch sind (Abbildung 26.24). Durch den Einsatz von RET lässt sich zwar die Ausgabequalität von Laserdruckern steigern, es ist aber auch mehr Arbeitsspeicher im Drucker erforderlich. Wird ein Speicherüberlauffehler gemeldet, lässt sich dieser manchmal durch Deaktivierung von RET beheben.

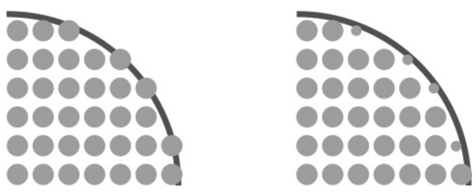


Abb. 26.24: Kantenglättungsverfahren füllen Lücken mit kleineren Druckpunkten, um Treppeneffekte zu vermeiden.

26.2.2 Laden

Nun wende ich mich dem physikalischen Teil des Druckvorgangs zu. Damit neue Bilder auf die Belichtungstrommel gezeichnet werden können, muss sie elektrisch geladen werden (Abbildung 26.25). Durch den Koronadraht oder die Ladewalze wird die gesamte Trommeloberfläche gleichmäßig negativ aufgeladen (mit ca. 600 bis 1.000 Volt).

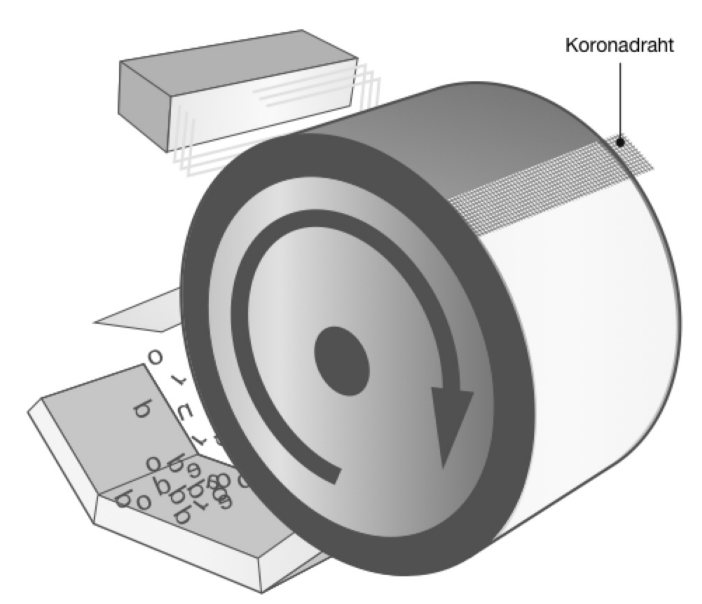


Abb. 26.25: Gleichmäßige negative Ladung der Trommel

26.2.3 Belichten

Mit einem Laser wird ein Positiv des Bildes auf die Trommeloberfläche geschrieben. Alle vom Laser belichteten Partikel auf der Trommel geben dabei den größten Teil ihrer negativen Ladung an die Trommel ab.

26.2.4 Entwickeln

Die Partikel mit geringerer negativer Ladung besitzen relativ zu den Tonerpartikeln eine positive Ladung, wodurch diese angezogen werden und so das entwickelte Bild erzeugen (Abbildung 26.26).

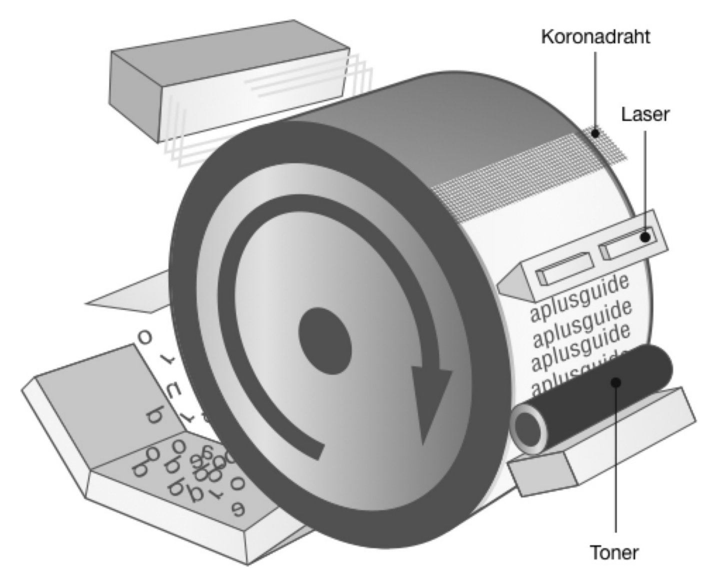


Abb. 26.26: Entwickeln des Bildes und Aufbringen des Toners

26.2.5 Übertragen

Der Drucker muss nun das Bild von der Trommel aufs Papier übertragen. Das Papier wird durch den unteren Koronadraht oder die Ladewalze mit einer positiven Ladung versehen. Wenn das Papier erst einmal eine positive Ladung besitzt, dann gehen die negativ geladenen Tonerpartikel von der Trommel zum Papier über. Zu diesem Zeitpunkt liegen die Partikel aber nur lose auf dem Papier auf und müssen noch dauerhaft damit verbunden werden.

26.2.6 Fixieren

Die Tonerpartikel sind vom Papier angezogen worden, weil dieses durch den unteren Koronadraht bzw. durch die Ladewalze positiv geladen wurde. Wäre der Vorgang hier beendet, würden die Tonerpartikel vom Papier abfallen, sobald Sie es in die Hand nehmen. Da Tonerpartikel größtenteils aus Kunststoff bestehen, können sie mit dem Papier verschmolzen werden. Zwei Rollen, von denen eine (die Heizrolle) mit einem nicht haftenden Material beschichtet ist, verschmelzen den Toner mit dem Papier, wodurch er dort permanent fixiert wird. Schließlich wird die positive Ladung des Papiers vom Entstatisierer entfernt (Abbildung 26.27). Wenn die Seite fertig bedruckt ist, wird sie vom Drucker ausgeworfen, und der Vorgang beginnt nach der physischen und elektrischen Reinigung des Druckers von vorn.

Vorsicht

Die Heizrolle wird heiß genug, um bestimmte Plastikmaterialien schmelzen zu können, wie z.B. Overhead-Folien. Dadurch kann der Laserdrucker beschädigt werden (die Garantie verfällt dabei). Achten Sie also darauf, dass Sie nur speziell für Laserdrucker geeignete Folien und beschichtete Papiersorten verwenden!

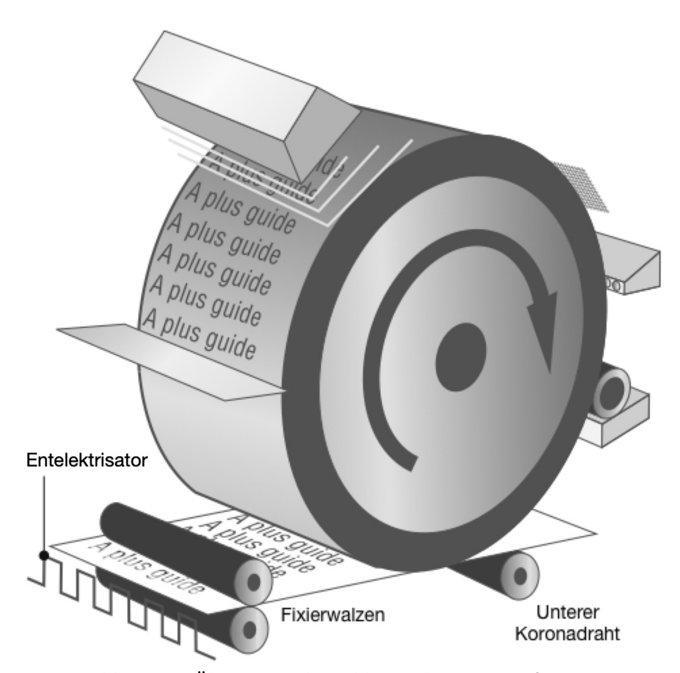


Abb. 26.27: Übertragen des Bildes und Fixieren auf Papier

26.2.7 Reinigen

Der Druckvorgang endet mit der physischen und elektrischen Reinigung der Belichtungstrommel (Abbildung 26.28).

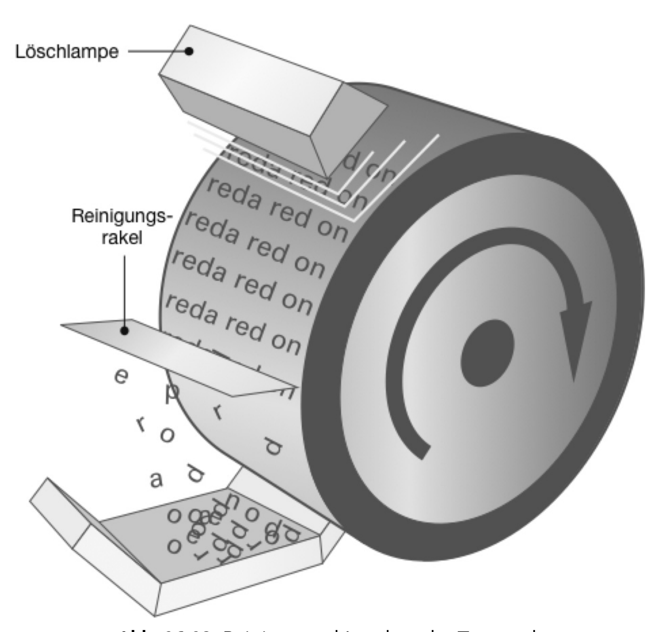


Abb. 26.28: Reinigen und Löschen der Trommel

Vor dem Drucken einer neuen Seite muss die Trommel wieder in einen sauberen Zustand zurückversetzt werden. Die nach dem letzten Druck verbliebenen Tonerreste müssen entfernt werden. Diese Aufgabe übernimmt üblicherweise ein Abstreifgummi (Reinigungsrakel), das den Toner von der Trommeloberfläche wischt. Wenn Partikel auf der Trommel haften bleiben, finden sich diese als zufällig verstreute Sprenkel und Streifen auf dem nächsten Blatt wieder. Bei der physischen Reinigung wird der übrige Toner entweder in einem Auffangbehälter gesammelt oder wieder in das Tonerreservoir der Kartusche zurückgeleitet. Die physische Reinigung muss mit großer Vorsicht erfolgen. Beschädigungen der Trommel führen dauerhaft zu Flecken oder Streifen auf allen nachfolgenden Druckseiten.

Der Drucker muss auch elektrisch »gereinigt« werden. Eine oder mehrere Löschlampen bombardieren die Oberfläche der Trommel mit Licht der entsprechenden Wellenlänge, wodurch die Oberflächenladungen vollständig entfernt werden und über die geerdete Trommel abfließen. Nach dem Reinigungsprozess sollten sich auf der elektrisch neutral geladenen Trommel keine Tonerpartikel mehr befinden.

Hinweis

Farblaserdrucker verwenden vier verschiedene Tonerfarben (Zyan, Magenta, Gelb und Schwarz) für ihre Ausdrucke. Die meisten Modelle verwenden vier Durchgänge für die Seiten, wobei bei jedem Durchgang eine Farbe aufgetragen wird, um die gewünschten Ergebnisse zu erzielen, während andere alle Farben auf einem speziellen Band unterbringen und sie dann in einem Durchgang auf die Seite übertragen. In einigen Fällen verwendet der Drucker vier separate Tonerkartuschen und vier Laser für die vier Tonerfarben, und in anderen legt der Drucker einfach eine Farbe nach der anderen auf derselben Trommel ab und reinigt sie nach jedem der vier Durchgänge für jede Seite.

26.3 Installation eines Multifunktionsgeräts

Die Installation eines Multifunktionsgeräts unterscheidet sich deutlich von derjenigen eines monofunktionalen Geräts. Für den Benutzer gestaltet sich der Vorgang aufgrund der Komplexität von Multifunktionsgeräten ziemlich umständlich.

Erstens werden die meisten Multifunktionsgeräte per USB oder über eine drahtlose Verbindung eingebunden, Sie müssen hier also eine Entscheidung treffen. Zweitens müssen Sie für die verschiedenen Funktionen des Multifunktionsgeräts Treiber installieren. Anfangs scheint das unproblematisch zu sein, denn Sie können ja die dem Gerät beiliegende Treiber-CD verwenden und die Software auf dem Betriebssystem Ihrer Wahl installieren.

Dieser Vorgang kann jedoch aus mehreren Gründen schnell zu einem ziemlichen Durcheinander führen. Die Treiber auf der mitgelieferten CD sind oft veraltet und die Installation der einzelnen Treiber durchzuführen kostet nicht nur Zeit, sondern auch Nerven. Noch schlimmer ist allerdings, dass die Hersteller häufig unglaublich schlechte Programme mitinstallieren, die irgendeine Funktion des Geräts »unterstützen« sollen, z.B. ein Werkzeug zur Verwaltung von Fotos, das den Rechner fast komplett lahmlegt und um einiges schlechter funktioniert als leicht verfügbare Dienste oder Programme wie Adobe Lightroom (nicht kostenlos, aber zu einem vernünftigen Preis erhältlich).

Drittens haben Sie es mit einem wirklich sehr komplexen Gerät zu tun, das auf äußerst interessante Weise ausfallen kann. Der Aufwand für die Wartung und Fehlerbehebung nimmt aufgrund der reinen Anzahl der zu berücksichtigenden Optionen völlig neue Dimensionen an, von Tintenfüllständen über die Mechanik des Scanners bis hin zu hartnäckig nicht funktionierenden Telefonleitungen. Das alles gehört zwar eigentlich nicht zur Installation, dennoch lassen sich viele Probleme vermeiden, wenn man bei der Installation nach Gerätekategorien getrennt vorgeht.

Sie und Ihre Kunden fahren viel besser, wenn Sie, anstatt sich auf die Funktionsvielfalt von Multifunktionsgeräten zu konzentrieren, die verschiedenen Funktionen als eigenständig betrachten. Nehmen Sie das Gerät beispielsweise in Gedanken auseinander und installieren Sie einen Drucker, einen Scanner, einen Kopierer und ein Faxgerät. Geben Sie die einzelnen Teile nach Bedarf im Netzwerk frei.

Aktualisieren Sie die Treiber der verschiedenen Komponenten getrennt voneinander. Stellen Sie sich die einzelnen Funktionen als separate Geräte vor, um die Fehlersuche zu erleichtern. Wenn z.B. die Druckausgabe nicht funktioniert, sollten Sie nur die Druckeraspekte des Multifunktionsgeräts betrachten. Sie brauchen sich nicht um die Scanner-, Kopierer- oder Fax-Merkmale zu kümmern.

Im nächsten Abschnitt geht es um die Installation von monofunktionalen Geräten, vornehmlich um Drucker. Das ist nämlich das, was die CompTIA A+-Prüfungen von Ihnen verlangen und womit Sie in der Praxis hauptsächlich zu tun haben werden.

26.3.1 Druckerinstallation unter Windows

Sie sollten sich zunächst die Zeit nehmen, um zu verstehen, wie Windows Druckvorgänge handhabt, und sich dann damit befassen, wie man unter diesen Betriebssystemen Drucker installiert, konfiguriert und deren Probleme behebt.

Wichtig

Die A+-Prüfungen der CompTIA fragen Sie nach der Installation und Fehlersuche bei Druckern, deshalb sollten Sie diese Abschnitte aufmerksam lesen!

Aus der Sicht von Windows ist ein Drucker kein physisches Gerät. Es handelt sich dabei um ein *Programm*, das einen oder mehrere physische Drucker steuert. Der physische Drucker wird als *Druckgerät* bezeichnet (obwohl ich größtenteils weiterhin den Begriff »Drucker« verwende). Es gibt weiterhin Druckertreiber und Druckerwarteschlange, aber unter Windows sind sie in den eigentlichen Drucker integriert (Abbildung 26.29). Durch dieses Schema kann Windows äußerst flexibel mit Druckern umgehen. Beispielsweise kann ein Drucker mehrere Druckgeräte unterstützen, sodass er sich wie ein Druckerserver verhalten kann. Wenn ein Druckgerät ausfällt, leitet der Drucker die Ausgabe automatisch auf ein funktionierendes Druckgerät um.

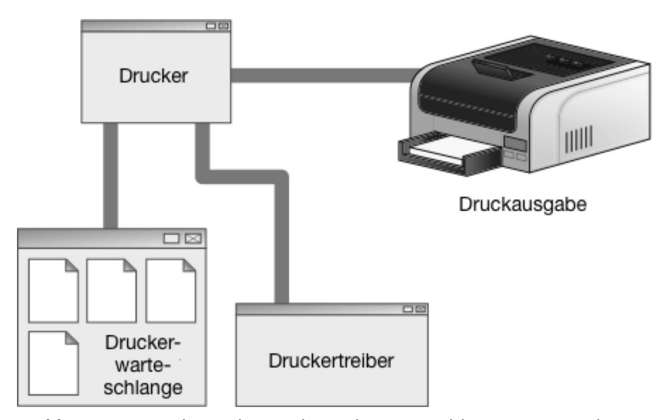


Abb. 26.29: Druckertreiber und Druckerwarteschlage unter Windows

Die allgemeine Vorgehensweise bei Installation, Konfiguration und Fehlersuche von Druckern ist unter allen modernen Windows-Versionen grundsätzlich gleich. Nachfolgend finden Sie die Beschreibung einer typischen Druckerinstallation. Ich werde dabei gegebenenfalls auf die kleinen Unterschiede zwischen Windows 7 und 8/8.1/10 hinweisen. Die Einrichtung eines Druckers ist schon fast beängstigend einfach. Die meisten Drucker werden automatisch erkannt (PnP – Plug&Play), sodass sich die Installation eines Druckers auf dessen Anschluss und das Laden des gegebenenfalls erforderlichen Treibers beschränkt. Bei USB-Druckern wartet Windows noch nicht einmal darauf, dass Sie etwas unternehmen, sondern installiert den Drucker nach dem Anschließen automatisch. Wenn das

System den Drucker unter Windows 7/8/8.1 nicht erkennnt, öffnen Sie in der Systemsteuerung das Applet GERÄTE UND DRUCKER. Wie Sie sich wohl bereits denken können, wird ein neuer Drucker über das Symbol DRUCKER HINZUFÜGEN bzw. NEUER DRUCKER installiert. Anschließend wird der Assistent DRUCKER HINZUFÜGEN gestartet.

In Windows 10 können Sie zwar auch die Systemsteuerung verwenden, die meisten Benutzer werden es aber vorziehen, für die Einrichtung das einfachere EINSTELLUNGEN|GERÄTE|DRUCKER UND SCANNER zu benutzen (Abbildung 26.30). Klicken Sie auf DRUCKER ODER SCANNER HINZUFÜGEN, um verfügbare Geräte anzuzeigen.

Hinweis: Standardbenutzer und Drucker

Standardbenutzer, also Benutzer ohne Administratorrechte, können in Windows problemlos einen Drucker installieren. Der Benutzer kann zum Drucken auch einen der vorinstallierten Druckertreiber verwenden.

Wenn der Benutzer allerdings versucht, Software oder Treiber zu installieren, die auf einem optischen Laufwerk gespeichert sind oder aus dem Internet heruntergeladen wurden, dann spielt Windows nicht mit. Dafür sind Administratorrechte erforderlich.

Falls Sie hier nicht weiterkommen, beispielsweise weil Mitarbeiter auf den vom Unternehmen bereitgestellten Laptops zu Hause Drucker installieren wollen, können Sie das Problem umgehen. Microsoft empfiehlt, die Gruppenrichtlinie für die Installation von Druckertreibern zu ändern, sodass Benutzern ohne Administratorrechte die Installation von Druckertreibern gestattet ist.

Eine ausführliche Anleitung finden Sie bei Bedarf unter `https://technet.microsoft.com`. Zu Gruppenrichtlinien komme ich in Kapitel 27.

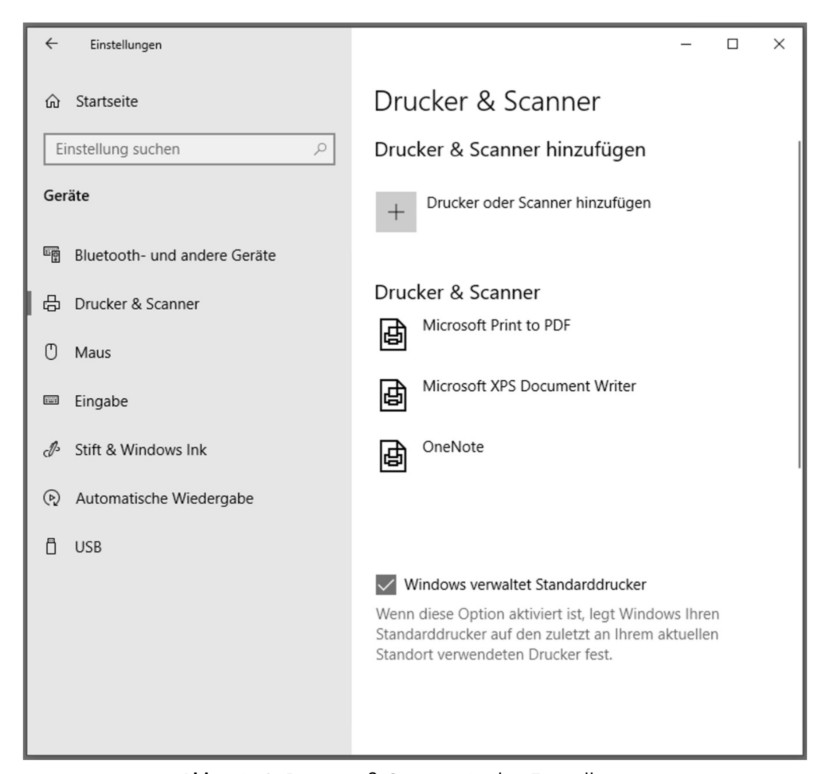


Abb. 26.30: DRUCKER & SCANNER in den Einstellungen

Der Assistent erlaubt die Installation eines lokalen Druckers oder eines Netzwerkdruckers. Diese Unterscheidung ist allerdings etwas irreführend. Windows unterteilt die Druckerinstallation in zwei Bereiche: direkt an einem PC angeschlossene Drucker (Ihr lokaler PC oder ein anderer PC im Netzwerk) und eigenständige Drucker, die mit einem Switch oder Router verbunden sind. Nun sollte man meinen, dass die Unterscheidung zwischen lokalen und Netzwerkdruckern eine sinnvolle Aufteilung wäre, aber so ist es leider nicht. Betrachten wir beide Methoden genauer, damit Sie erfahren, wann welche anzuwenden ist.

Installation lokaler Drucker

Auf den ersten Blick könnte man denken, dass mit der lokalen Druckerinstallation auch normale USB-Drucker installiert werden, aber denken Sie daran, dass Windows diese automatisch erkennt und installiert (wie alle anderen PnP-Drucker auch). Wozu ist sie dann gut? Sie wird vornehmlich dazu verwendet, Drucker mit paralleler Schnittstelle oder eigenständige Netzwerkdrucker, die eine IP-Adresse besitzen, zu installieren. Bei der Verwendung moderner Windows-Versionen und aktueller Drucker sollte es nicht nötig sein, zur Installation eines eigenständigen Netzwerkdruckers eine IP-Adresse angeben zu müssen, es bietet sich aber als brauchbare Alternative an, falls Windows den Drucker auf anderem Wege nicht erkennt.

Wenn Sie einen eigenständigen Netzwerkdrucker installieren möchten, können Sie die IP-Adresse oder den Hostnamen verwenden. Klicken Sie in Windows 7 auf EINEN LOKALEN DRUCKER HINZUFÜGEN. Wählen Sie im Einblendmenü NEUEN ANSCHLUSS ERSTELLEN den Punkt STANDARD-TCP/IP-PORT aus und klicken Sie auf WEITER. Geben Sie hier die IP-Adresse ein. In Windows 8/8.1/10 ist es sogar noch einfacher: Wenn Windows Ihren Drucker nicht automatisch erkennt, klicken Sie einfach auf DER GEWÜNSCHTE DRUCKER IST NICHT AUFGELISTET und wählen dann DRUCKER UNTER VERWENDUNG EINER TCP/IP-ADRESSE ODER EINES HOSTNAMENS HINZUFÜGEN. In Windows 10 bieten die Einstellungen und die Systemsteuerung die gleichen Optionen.

Ob Sie einen USB-Anschluss oder eine TCP/IP-Adresse verwenden, spielt keine Rolle, Sie müssen den richtigen Treiber in jedem Fall von Hand auswählen (Abbildung 26.31). Windows enthält eine Menge Druckertreiber, Sie können aber auch auf die Option DATENTRÄGER zurückgreifen, um die dem Drucker beiliegende Treiber-CD zu verwenden. Wenn Sie das tun möchten, benötigen Sie zum Fortfahren Administratorrechte. Mit der Schaltfläche WINDOWS UPDATE können Sie im Internet nach den neuesten Treiberversionen suchen.

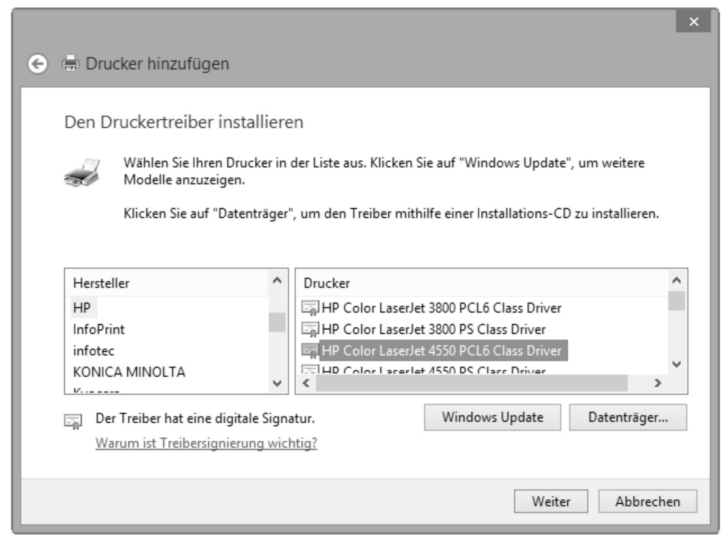


Abb. 26.31: Auswahl des Druckertreibers

Nach dem Klick auf WEITER werden Sie gefragt, ob der neue lokale Drucker als Standarddrucker eingerichtet werden soll und ob Sie ihn im Netzwerk freigeben möchten. Sie können also tatsächlich einen eigenständigen Netzwerkdrucker über Ihren PC mittels Druckerfreigabe im Netzwerk bereitstellen, der dann allerdings nicht mehr zur Verfügung steht, sobald Sie Ihren Rechner abschalten. Schließlich werden Sie aufgefordert, eine Testseite auszudrucken, um zu gewährleisten, dass alles funktioniert. Und fertig!

Wichtig

Druckerfreigaben unter Windows sind nicht die einzige Möglichkeit, Drucker gemeinsam zu nutzen. Apples *AirPrint* kann in Kombination mit dem *Bonjour Druckdienst* (den Sie separat oder zusammen mit iTunes installieren müssen) dazu verwendet werden, einen an einem Windows-System angeschlossen Drucker AirPrint-kompatiblen Geräten bereitzustellen, auf denen macOS oder iOS läuft.

Installation von Netzwerkdruckern

Erstaunlicherweise ist die Einrichtung von Netzwerkdruckern kaum aufwendiger als die Installation lokaler Drucker. Wenn Sie versuchen, einen Netzwerkdrucker einzurichten, sucht der Assistent zum Hinzufügen von Druckern im lokalen Netzwerk nach verfügbaren Druckern (Abbildung 26.32). Meistens funktioniert das auch und der gesuchte Drucker wird in einer Liste angezeigt. Nach Auswahl eines Druckers und einem Klick auf WEITER sucht Windows nach passenden Treibern. Gegebenenfalls können Sie aus einer Liste verfügbarer Treiber einen auswählen oder die zusammen mit dem Drucker gelieferten Installationsmedien verwenden. In beiden Fällen ist die Arbeit für Sie damit erledigt.

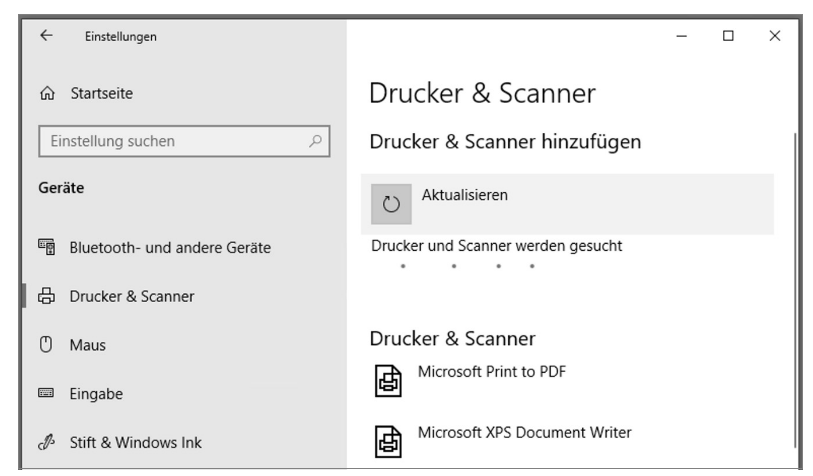


Abb. 26.32: Liste der im Netzwerk verfügbaren Drucker

Hinweis

Erinnern Sie sich an die Druckerfreigabe aus Kapitel 19? Hier sehen Sie die andere Hälfte einer Freigabe. Wenn Sie einen freigegebenen Drucker auf Ihrem System installieren, können Sie diesen Ihrerseits freigeben! Windows betrachtet den Drucker als den Ihren und Sie können mit ihm anstellen, was Sie möchten, inklusive ihn freigeben.

Falls Windows Ihren Netzwerkdrucker nicht erkennt, müssen Sie ihn von Hand einrichten. Dafür gibt es in jeder Windows-Version verschiedene Methoden, die davon abhängig sind, ob Sie Mitglied einer Domäne oder einer Arbeitsgruppe sind.

Falls Sie sich in einer Arbeitsgruppe befinden, können Sie sich die Netzwerkdrucker anzeigen lassen und sich mit einem davon unter Verwendung der URL bzw. der IP-Adresse oder des Hostnamens verbinden (Abbildung 26.33). In einer Domäne stehen dieselben Möglichkeiten zur Verfügung, allerdings können Sie bei der Anzeige der Netzwerkdrucker in einer Domäne Suchparameter angeben (Fähigkeiten des Druckers, Ort des Druckers usw.). Wenn Sie den passenden Drucker gefunden haben, werden Sie möglicherweise aufgefordert, einen Treiber anzugeben. Verwenden Sie dazu die bereits beschriebenen Methoden und schon sind Sie fertig.

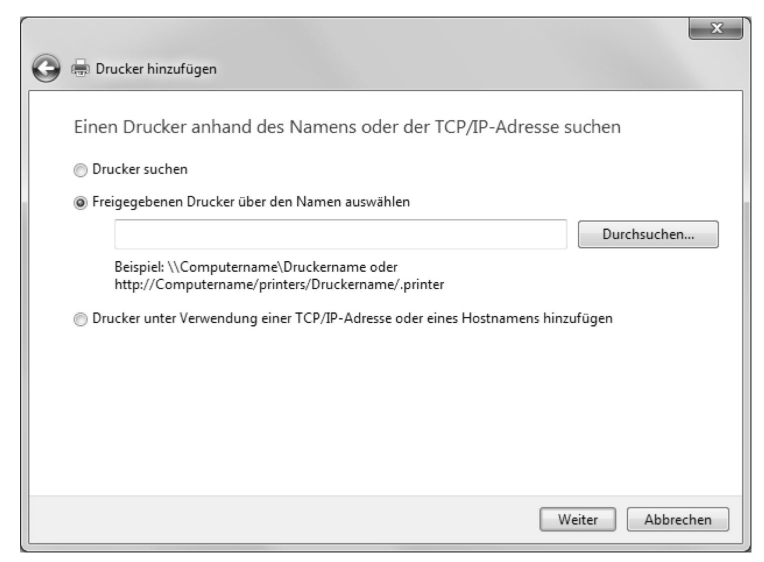


Abb. 26.33: Optionen bei der Auswahl des Netzwerkdruckers

Hinweis

Wenn Sie Mitglied einer Heimnetzgruppe sind und die Druckerfreigabe aktiviert ist, werden alle an der Heimnetzgruppe angeschlossenen Drucker automatisch für Sie freigegeben. Das gilt aber nur für Windows 7/8/8.1. Die ersten Versionen von Windows 10 unterstützten Heimnetzgruppen noch, bei aktuellen Versionen ist das jedoch nicht mehr der Fall.

Beachten Sie, dass Netzwerkdrucker in Windows nicht immer so erscheinen, wie sie eigentlich physisch verbunden sind. Denken Sie an ein Netzwerk mit drei Rechnern. An Annas Computer ist via USB ein Drucker angeschlossen, während Bernd und Carola über keinen Drucker verfügen. Es gibt aber einen zweiten Drucker, der per Ethernet direkt am Router angeschlossen ist. Bernd hat auf seinem Rechner den direkten Zugriff auf den Drucker via IP-Adresse eingerichtet. Nachdem er das erledigt hat, kann er diesen Drucker für den Rest des Netzwerks freigeben, obwohl dieser gar nicht direkt an seinem Computer angeschlossen ist. Windows ist es egal, wo sich der Drucker befindet. Die Freigabe von lokalen und Netzwerkdruckern geschieht auf dieselbe Weise, weil Windows beide Drucker als auf Bernds System installiert betrachtet und er daher auch die Kontrolle darüber besitzt. Anna und Bernd haben also beide Drucker freigegeben. Wenn Carola nun nach einem Netzwerkdrucker sucht, sieht es für sie so aus, als ob der Netzwerkdrucker an Bernds Computer angeschlossen wäre.

Abbildung 26.34 zeigt ein typisches Fenster DRUCKER & SCANNER für ein System mit vorinstallierten Druckern. Beachten Sie die Kennzeichnung STANDARD rechts neben dem Symbol des Druckers, die darauf hinweist, dass es sich bei diesem um den Standarddrucker handelt. Wenn Sie mehrere Drucker besitzen, können Sie den Standarddrucker dadurch festlegen, dass Sie den Drucker auswählen, auf VERWALTEN klicken und dann die Option ALS STANDARD anklicken.

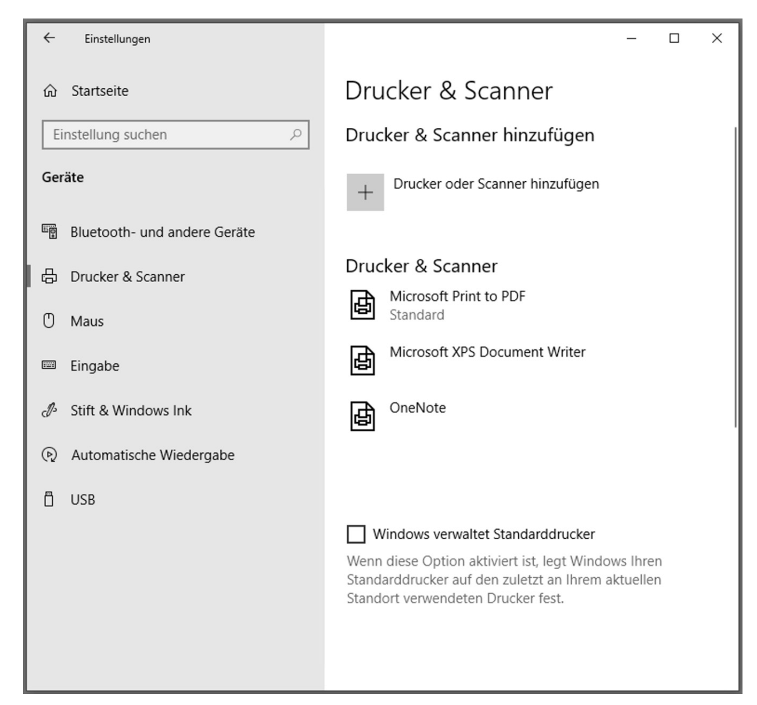


Abb. 26.34: Standarddrucker im Fenster DRUCKER & SCANNER

Neben der zuvor vorgestellten Installation echter Drucker und der dazu passenden Treiber werden manchmal auch *Druckeremulationen* installiert. Bei der Druckeremulation ersetzt man einfach den Treiber eines Druckers, der speziell für diesen erstellt wurde, durch einen anderen Treiber, wie z.B. den für ein baugleiches Druckermodell eines anderen Herstellers oder ein kompatibles Vorgängermodell desselben Herstellers. Auf die Druckeremulation greift man gewöhnlich in zwei Fällen zurück. Erstens werden einige neue Drucker ohne eigene Treiber geliefert. Stattdessen emulieren diese Drucker einen bekannten Drucker (z.B. einen HP LaserJet 4) und arbeiten einwandfrei mit dem entsprechenden Druckertreiber zusammen. Zweitens kann man natürlich auf die Emulation zurückgreifen, wenn die Datenträger mit Treibern nicht vorliegen oder abhandengekommen sind. Auf meinem Rechner sind drei verschiedene Druckermodelle (HP LaserJet und Epson-Tintenstrahler) installiert, da ich weiß, dass ich mit diesen Druckertreibern auf nahezu allen Druckern ausdrucken kann. Einige Drucker müssen in einen Emulationsmodus umgeschaltet werden, damit sie mit einem anderen als dem eigenen Treiber klarkommen.

1002

Sie können sich sicher denken, dass sich die Einrichtung von Druckern und Multifunktionsgeräten in Unternehmensumgebungen und im SOHO-Bereich voneinander unterscheidet. Hier ist ein Beispiel. Bei der Bayland Widgets Corporation gibt es 30 Benutzer, die zwei hochwertige Farblaserdrucker, zwei sehr schnelle Schwarz-Weiß-Laserdrucker, ein Multifunktionsgerät (vornehmlich zum Scannen und Kopieren, aber auch zum Drucken) und drei Tintenstrahldrucker gemeinsam nutzen. Die Drucker und das Multifunktionsgerät stehen an verschiedenen Standorten und werden durch einen einzigen Druckerserver verwaltet.

Um nicht auf jedem einzelnen Client-Rechner die Netzwerkdrucker installieren zu müssen, verwendet der Administrator Tony Windows-Gruppenrichtlinien, um den 30 Arbeitsplatzrechnern (und einigen

Laptops) die richtigen Drucker zuzuordnen. Wenn die Benutzer sich morgens anmelden, weist die Gruppenrichtlinie allen Arbeitsplatzrechnern und Laptops das Multifunktionsgerät und den nächstgelegenen Farblaserdrucker zu. Die hochwertigen Tintenstrahldrucker und die schnellen Schwarz-Weiß-Laserdrucker werden allerdings nur den Rechnern der Marketingabteilung bzw. der Buchhaltung zugewiesen. Alles funktioniert automatisch, und bei Bedarf werden die richtigen Treiber geladen.

Wichtig

Rechnen Sie in der CompTIA A+Prüfung 1002 mit Fragen, bei denen Sie eine Auswahl zwischen normaler Druckerfreigabe und gemeinsamer Nutzung von Druckern über einen Druckerserver treffen müssen. Der wesentliche Unterschied ist die Größe des Netzwerks. Die gemeinsame Nutzung eines Multifunktionsgeräts oder eines Druckers in einem SOHO-Netzwerk ist ziemlich einfach, ebenso wie die Einrichtung einer Druckerfreigabe im Netzwerk. Wenn die Anzahl der Geräte zunimmt, kann die Verwaltung vieler Arbeitsplatzrechner und Drucker/Mufus aber schnell sehr mühsam werden, wenn man keine Gruppenrichtlinie dafür verwendet, die für viele Computer oder Benutzer gilt.

Sie könnten die Automatisierung in einer Active-Directory-Domäne auch, wie in Kapitel 19 erläutert, durch ein Anmeldeskript automatisieren. Achten Sie darauf, wenn ein Anmeldeskript eine Antwortmöglichkeit ist, eine Gruppenrichtlinie aber nicht.

Wir betrachten Gruppenrichtlinien in Kapitel 27. Die Zuordnung von Multifunktionsgeräten und Druckern auf diese Weise ermöglicht eine viel schnellere Aktualisierung, Verteilung von Änderungen und so weiter.

Wichtig

Neben dem Applet GERÄTE UND DRUCKER gibt es in Windows die DRUCKVERWALTUNG, die es Ihnen erlaubt, alle mit Ihrem PC oder per Netzwerk verbundenen Drucker und sämtliche Druckertreiber anzuzeigen und zu bearbeiten. Sie können damit außerdem auch die im Netzwerk verfügbaren Windows-Druckerserver verwalten. Viele der Funktionen der DRUCKVERWALTUNG gehen über die Anforderungen der CompTIA A+-Prüfungen weit hinaus. Sie sollten aber wissen, dass dadurch die Handhabung der Standarddrucker in Windows zentralisiert und in einigen Fällen sogar erweitert wird. Sie finden sie in der Systemsteuerung unter VERWALTUNG|DRUCKVERWALTUNG.

1001

26.3.2 Druckeinstellungen konfigurieren

Nachdem Ihr Drucker installiert ist, ist es eine gute Idee, sich mit den Einstellungen beim Drucken zu befassen, auf die Sie im Applet GERÄTE UND DRUCKER durch einen Rechtsklick auf den gewünschten Drucker und Auswahl von DRUCKEINSTELLUNGEN zugreifen können. Hier können Sie einstellen, wie Ihr Drucker Ihre Dokumente zu Papier bringt. Sie müssen sich aber darüber im Klaren sein, dass die verfügbaren Einstellungen von den Features Ihres Druckers oder Multifunktionsgeräts abhängig sind. Sehen wir uns also einige der Einstellungen an, die Sie höchstwahrscheinlich auch vorfinden werden.

Layout

Die Einstellungen, die Sie vermutlich hin und wieder ändern werden, betreffen das Layout. Sie steuern, wie der Drucker ermittelt, was er wo druckt.

- **Beidseitig drucken**: Diese Einstellung legt fest, ob und wie beide Seiten eines Blatts bedruckt werden. Normalerweise werden die Blätter der Reihe nach von vorn und hinten bedruckt, es gibt jedoch auch Optionen zum Broschürendruck.

- **Seiten pro Blatt**: Hier geben Sie an, wie viele Seiten auf einem Papierblatt ausgegeben werden sollen.
- **Ausrichtung**: Die Ausrichtung legt fest, ob im Hoch- oder Querformat gedruckt wird.
- **Größenveränderungsoptionen/Skalierung**: Diese Einstellung, nicht zu verwechseln mit Seiten pro Blatt, dient dazu, große Dokumente auf einer einzelnen Seite oder aber kleine Dokumente seitenfüllend auszugeben.
- **Spiegelverkehrt/Seitenverkehrt** : Gibt das Dokument spiegelverkehrt aus. Das kann sinnvoll sein, wenn auf Umdruckpapier oder Overhead-Folie gedruckt wird.

Papier

Viele der Druckeinstellungen beziehen sich auf die Art des Papiers, auf dem gedruckt wird und wo es sich befindet (sofern der Drucker mehrere Papierfächer besitzt).

- **Papierformat**: Stellen Sie das Papierformat ein oder verwenden Sie eine benutzerdefinierte Größe.
- **Papiertyp**: Gibt an, wie dick das Papier ist, ob es beschichtet ist oder ob es sich um einen speziellen Typ wie Briefumschläge oder selbstklebende Etiketten handelt.
- **Papiereinzug/Quelle**: Wählen Sie ein Papierfach aus (falls vorhanden) oder verwenden Sie die manuelle Zufuhr. Der Drucker wartet dann darauf, dass Sie ein Papierblatt einlegen. Sie ist auch nützlich, wenn das zu bedruckende Papier nicht in das Papierfach passt.

Qualität

Darüber hinaus gibt es Einstellungen, die sich auf die Qualität auswirken und nicht selten den Tinten- bzw. Tonerverbrauch erwähnen und daher nicht wie die anderen erwähnten Einstellungen auf der Registerkarte PAPIER/QUALITÄT zu finden sind:

- **Druckqualität**: Legt die Auflösung in dpi fest.
- Bei manchen Druckern können Sie zwischen verschiedenen Voreinstellungen auswählen, die den Druck für die Ausgabe von Text oder Grafik optimieren. Oftmals können Sie diese auch selbst konfigurieren.
- **Sparmodus/Eco-Modus**: Viele Drucker bieten einen Sparmodus an, der weniger Tinte bzw. Toner verwendet. Das ist wirtschaftlicher und schont die Umwelt.

Weitere Einstellungen

Manche Drucker verfügen über Optionen, die zwar selten gebraucht werden, dann jedoch sehr nützlich sind.

- **Wasserzeichen**: Durch die Ausgabe eines Wasserzeichens, einer blassen Markierung, die auf jeder Seite gedruckt wird, können Sie beispielsweise ein Dokument als Entwurf kennzeichnen, um es von der endgültigen Version zu unterscheiden.
- **Kopf- und Fußzeilen**: Sie enthalten Informationen wie die Seitenzahl, oder wann und von wem das Dokument gedruckt wurde.
- **Kollationieren**: Hier können Sie festlegen, in welcher Reihenfolge die Seiten eines Dokuments ausgegeben werden, wenn Sie mehrere Kopien davon drucken. Wenn Sie zehn Kopien drucken, wird die erste Seite zehn Mal gedruckt, dann zehn Mal die zweite Seite usw. Ansonsten wird das Dokument zehn Mal zusammenhängend ausgegeben.

26.3.3 Optimierung der Druckleistung

Der erste Schritt zu einer qualitativ hochwertigen Ausgabe ist zwar ein vernünftiger Drucker, aber Ihre Ausdrucksqualität ist noch von weiteren Faktoren abhängig. Wenn Sie schon einmal stundenlang an einem digitalen Foto auf dem Bildschirm gearbeitet haben, nur um anschließend festzustellen, dass

der Ausdruck dann dunkler als erwartet ist, haben Sie eine wichtige Entdeckung gemacht. Das, was Sie auf dem Bildschirm sehen, stimmt möglicherweise nicht mit dem Ausdruck überein, wenn beide Geräte nicht ordnungsgemäß kalibriert sind.

Wichtig

Kalibrieren ist ein allgemeiner Ausdruck für die Korrektur der Unterschiede zwischen tatsächlicher und gewünschter Arbeitsweise eines Geräts. Die verschiedensten Geräte müssen kalibriert werden, aber die Lernziele der CompTIA konzentrieren sich auf die Kalibrierung von Tintenstrahl- und Laserdruckern. Dieser Abschnitt beschreibt nur eine Art der Kalibrierung, aber in den Abschnitten *Wartung von Tintenstrahldruckern* und *Wartung von Laserdruckern* finden Sie weitere Schritte, die bei der Kalibrierung erforderlich sind.

Bei der *Farbkalibrierung* wird mit spezieller Hardware ein ICC-Farbprofil (International Color Consortium) erstellt, eine Referenzdatei, die die Farbcharakteristik eines Geräts beschreibt. Das Betriebssystem nutzt dieses Profil, um Verschiebungen bei der Farbdarstellung zu korrigieren. Wenn der Monitor kalibriert ist, können Sie erkennen, dass irgendwelche Farbverschiebungen Teil des Fotos sind und nicht von der Darstellung auf dem Bildschirm verursacht werden.

Hinweis

Datacolor Spyder und X-Rite ColorMunki Display sind Geräte zur Farbkalibrierung von zwei der renommiertesten Hersteller solcher Hardware. (Ich verwende hauptsächlich Ersteres.) Beschaffen Sie sich so ein Gerät. Sie werden mit Ihren Ausdrucken sehr viel zufriedener sein. Hier sind die URLs: `http://www.datacolor.com` und `http://www.xrite.com`.

Richtig interessant wird der Einsatz von Farbprofilen, wenn auch der Drucker kalibriert wird. Wie beim Monitor sind dem Computer die Eigenheiten bei der Farbdarstellung eines bestimmten Druckers auf einer bestimmten Papiersorte bekannt. Wenn sowohl Bildschirm als auch Drucker richtig kalibriert sind und Farbprofile verwenden, sollte die farbliche Darstellung auf dem Bildschirm mit dem Ausdruck übereinstimmen. Auch auf der Installations-CD eines Druckers befinden sich manchmal Farbprofile, aber Sie können auch benutzerdefinierte Profile erstellen oder kaufen. Windows enthält mit *WCS* (*Windows Color System*) ein Hilfsmittel zum Erstellen von Farbprofilen für die Nutzung mit verschiedenen Geräten. WCS basiert auf einem neueren Standard, den Microsoft *CITE* (*Color Infrastructure and Translation Engine*) nennt.

26.3.4 Handhabung allgemein zugänglicher Drucker

Sie haben nun verschiedene Möglichkeiten kennengelernt, wie man vernetzte Drucker und Multifunktionsgeräte gemeinsam nutzen kann. Mit der Einrichtung allein ist es aber noch nicht getan, denn auch der Netzwerksicherheit und der Privatsphäre müssen Beachtung geschenkt werden.

Netzwerksicherheit

Der leichte Zugang, der kabelgebundene oder drahtlos vernetzte Drucker so nützlich macht, stellt gleichzeitig ein erhebliches Risiko dar, denn sie sind anfällig für Angriffe aus dem LAN, schlimmstenfalls sogar für Angriffe aus dem Internet. Die Absicherung vernetzter Drucker oder Multifunktionsgeräte geht zwar über den Rahmen dieses Buches hinaus, es ist jedoch wichtig, sich der möglichen Gefahren bewusst zu sein, die mit diesen Geräten verbunden sein können. Dass im Ausgabefach herumliegende Dokumente einer gewissen Gefahr ausgesetzt sind, liegt auf der Hand. Aber da die Sicherheitsaspekte bei diesen Geräten oft vernachlässigt werden, können sie auch Ausgangspunkt für Angriffe aus dem Netzwerk sein.

Vertrauliche Daten

Wenn man einen Moment darüber nachdenkt, wird klar, dass in den meisten Unternehmen und Organisationen eine Menge vertraulicher Daten durch Drucker und Multifunktionsgeräte ausgegeben werden, insbesondere in Schulen und Krankenhäusern, denn hier ist die Handhabung vertraulicher Daten besonders wichtig. Wenn all diese Informationen den Drucker durchlaufen, muss gewährleistet sein, dass Unbefugte nicht darauf zugreifen können. Unglücklicherweise enthalten viele dieser Geräte eine Festplatte oder andere Speichermedien, die zum Zwischenspeichern von Kopien der Dokumente verwendet werden, die gedruckt, gescannt, kopiert oder gefaxt werden. Je nach Gerät kann diese Funktion deaktiviert werden oder es gibt die Möglichkeit, den Zwischenspeicher regelmäßig automatisch bzw. von Hand zu löschen, um so den Schaden zu begrenzen, den eine Kompromittierung des Geräts verursachen würde. Außerdem ist es wichtig, diese Daten zu löschen, bevor das Gerät ausrangiert und entsorgt wird.

Wichtig

Die CompTIA verwendet dafür den Begriff Festplatten-Caching.

Das Deaktivieren dieser Funktion wäre ziemlich nutzlos, wenn jeder Benutzer des Geräts die Einstellung wieder ändern könnte. Netzwerkfähige Drucker ermöglichen es daher häufig, eine Benutzerauthentifizierung einzurichten. Wenn die Verwendung nur authentifizierten Benutzern gestattet ist und sie nur auf die erforderlichen Funktionen zugreifen dürfen, lassen sich dadurch viele der mit diesen Geräten einhergehenden Risiken vermeiden.

Auch wenn die Daten auf Ihrem Computer sicher sind, heißt das noch lange nicht, dass sie auch bei der Ausgabe auf Druckern oder Multifunktionsgeräten vor neugierigen Augen geschützt sind. Daher gibt es die Möglichkeit, Dokumente an das Gerät zu übermitteln, die jedoch erst dann ausgegeben werden, wenn sich der Benutzer direkt am Gerät authentifiziert. Die Benutzerauthentifizierung minimiert darüber hinaus die Gefahr, dass Unbefugte Dokumente scannen, kopieren oder als E-Mail versenden und so unbemerkt Dokumente stehlen können, indem sie das Original an Ort und Stelle belassen.

26.4 Fehlerbehebung bei Druckern

Drucker lassen sich nicht nur einfach einrichten, sondern arbeiten meist auch äußerst zuverlässig, sofern nur die richtigen Treiber installiert sind und der Drucker gut gewartet wird. Gelegentlich kommt es aber doch zu Druckerfehlern. Die häufigsten Windows-Druckprobleme und Probleme, die beim Einsatz spezieller Druckertypen auftreten können, werden wir uns nun ansehen.

Hinweis

Alle Drucker sind unterschiedlich. Lesen Sie in der Dokumentation Ihres Druckers nach, wie die hier beschriebenen Aufgaben durchgeführt werden.

26.4.1 Allgemeine Aspekte der Fehlersuche

Drucker aller Bauarten weisen einige allgemeine Probleme auf, wie beispielsweise dass Druckaufträge nicht ausgegeben werden, dass in merkwürdiger Größe gedruckt wird oder dass Ausdrucke fehlerhaft ausgerichtet sind. Andere Aspekte betreffen den Materialverbrauch, die gemeinsame Nutzung mehrerer Drucker oder den Absturz beim Einschalten. Wir werden diese allgemeinen Aspekte der Fehlersuche eingehender betrachten, werden aber erst einmal mit einem Überblick über die wichtigsten benötigten Werkzeuge beginnen.

Wichtig

Übersehen Sie das Naheliegende nicht! Viele Drucker besitzen Anzeigen, die Ihnen Fehlerhinweise liefern können. Viele Hersteller setzen Fehlercodes ein, um Probleme zu beschreiben. Die Fehlercodes können Sie im Druckerhandbuch oder auf der Website des Herstellers nachschlagen.

Die wichtigsten Werkzeuge

Bevor Sie mit der Arbeit an einem problematischen Drucker beginnen, benötigen Sie ein paar Werkzeuge. Neben den Standardwerkzeugen aus Ihrer Werkzeugtasche können Sie einige weitere druckerspezifische Hilfsmittel verwenden. Die folgenden sind praktisch:

- Ein Multimeter für die Suche nach elektrischen Problemen, wie beispielsweise defekten Wandsteckdosen
- Verschiedene Reinigungslösungen, wie z.B. Brennspiritus (denaturierter Alkohol)
- Einen Stab mit einem kleinen Magneten, um heruntergefallene Schrauben aus engen Gehäusenischen herauszufischen und eisenhaltigen Toner zu entfernen
- Eine CD oder ein USB-Speicherstick mit Testbildern zur Überprüfung der Druckqualität
- Ihre guten alten Kreuzschlitz- und Schlitzschraubendreher, um für alle Fälle gerüstet zu sein

Druckaufträge werden nicht ausgedruckt

Wenn der Drucker nach dem Anklicken der DRUCKEN-Schaltfläche gar nicht reagiert, sollten Sie zunächst alle möglichen offensichtlichen Fehlerquellen eliminieren. Ist der Drucker eingeschaltet? Ist er angeschlossen? Ist er online geschaltet? Zeigt er eine Fehlermeldung an? Befindet sich Papier im Einzugsschacht? Ist Ihr Computer online?

Wenn der Drucker eingeschaltet ist, zeigt er möglicherweise eine Fehlermeldung an. Für gewöhnlich zeigt ein Drucker an, wenn kein Papier vorhanden ist, ein Papierstau vorliegt oder wenn es zu einem Speicherüberlauf gekommen ist. Legen Sie in diesem Fall Papier nach, beseitigen Sie den Papierstau oder versuchen Sie, das Dokument in geringerer Qualität auszudrucken.

Wenn Sie keine Verbindung zum Drucker herstellen können, überprüfen Sie alle beteiligten Kabel, Anschlüsse und Stromversorgungen. Wenn alles in Ordnung zu sein scheint, sollten Sie nachsehen, ob der Drucker eine Fehlermeldung wie KEINE VERBINDUNG anzeigt (eventuell müssen Sie das entsprechende Menü anwählen, um den Verbindungsstatus anzuzeigen).

Wenn die Verbindung funktioniert, rufen Sie das Drucker-Applet Ihrer Windows-Version auf. Falls der Drucker nicht angezeigt wird, müssen Sie ihn mithilfe des Druckerinstallations-Assistenten erneut installieren.

Wenn Sie einen von einem anderen PC freigegebenen Drucker verwenden möchten, Windows aber eine »Zugriff verweigert«-Fehlermeldung zeigt, fehlen Ihnen offenbar die erforderlichen Zugriffsrechte. Suchen Sie den PC auf, der den Drucker freigibt, und überprüfen Sie auf der Registerkarte SICHERHEIT des EIGENSCHAFTEN-Dialogfelds des Druckers die Einstellungen. Stellen Sie sicher, dass Ihr Benutzerkonto den Drucker verwenden darf.

Wenn mit dem Drucker alles in Ordnung ist, sollten Sie einen Blick in die Druckerwarteschlange werfen. Den Status der Druckerwarteschlange können Sie feststellen, wenn Sie entweder das Symbol des Druckers im Applet DRUCKER oder das winzige Druckersymbol in der Taskleiste doppelklicken, sofern dieses dort vorhanden ist. Das ist allerdings beim Vorliegen von Problemen fast immer der Fall. Abbildung 26.35 zeigt die geöffnete Druckerwarteschlange.

Warteschlangen können leicht überlaufen oder wegen mangelnder Festplattenkapazität, zu vieler Druckaufträge oder tausend anderen Faktoren hakeln. In diesem Fenster werden alle noch ausstehenden Druckaufträge angezeigt. Hier können Sie einzelne Aufträge löschen, starten oder anhalten. Ich lösche üblicherweise nur die problematischen Druckaufträge und versuche den Ausdruck anschließend erneut.

Abb. 26.35: Die Druckerwarteschlange

Warteschlangen sind wirklich praktisch. Wenn der Drucker ausgeschaltet wird oder ausfällt, dann können Sie die Druckaufträge einfach in der Warteschlange lassen, bis der Drucker wieder eingeschaltet wird bzw. betriebsbereit ist. Wenn ein Drucker in absehbarer Zeit nicht verfügbar sein wird, dann können Sie den entsprechenden Druckauftrag einfach im Fenster der Druckerwarteschlange löschen und einen anderen Drucker ausprobieren.

Wenn Sie Probleme mit der Druckerwarteschlange haben, können Sie die entsprechenden Einstellungen ändern. Öffnen Sie das Applet GERÄTE UND DRUCKER, klicken Sie den betreffenden Drucker mit der rechten Maustaste an und wählen Sie EIGENSCHAFTEN. In dem Dialogfeld (Abbildung 26.36) markieren Sie das Optionsfeld DRUCKAUFTRÄGE DIREKT ZUM DRUCKER LEITEN und klicken auf OK. Anschließend senden Sie Ihren Druckauftrag erneut. Über dieses Dialogfeld können Sie auch einstellen, dass Druckaufträge sofort gestartet werden, wenn genügend Informationen vorliegen, um den Drucker anzusteuern, oder dass erst dann mit dem Drucken begonnen wird, wenn sich der gesamte Auftrag in der Warteschlange befindet.

Abb. 26.36: Einstellungen für die Druckerwarteschlange

Wenn das nicht weiterhilft, können Sie versuchen, den Dienst DRUCKERWARTESCHLANGE neu zu starten. Klicken Sie mit der rechten Maustaste auf das Startmenü und wählen Sie Computerverwaltung (Administratorrechte sind erforderlich). Doppelklicken Sie in der Spalte links auf DIENSTE UND

ANWENDUNGEN und dann auf DIENSTE. Suchen Sie nach dem Dienst DRUCKERWARTESCHLANGE, klicken Sie mit der rechten Maustaste darauf und wählen Sie BEENDEN. Sobald der Dienst beendet wurde, klicken Sie erneut mit der rechten Maustaste darauf und wählen STARTEN. Nun sollte das Drucken wieder funktionieren.

Eine weitere mögliche Ursache für einen nicht ausgeführten Druckauftrag kann sein, dass der Drucker einfach auf das richtige Papier wartet. Vor allem bei Laserdruckern gibt es Einstellungen und Sensoren, über die ihnen mitgeteilt wird, welche Papiergröße sich im Papierschacht befindet. Wenn ein Programm einen Druckauftrag für eine andere Papiergröße sendet und beispielsweise einen Standardumschlag bedrucken will, sich im Papierschacht aber nur A4-Papier befindet, dann nimmt der Drucker seine Arbeit normalerweise gar nicht auf, sondern wartet erst einmal darauf, dass jemand die Papierkassette wechselt oder das für den Druckauftrag benötigte Papier manuell einlegt. Wenn Sie am Drucker die Taste »OK« oder »Fortsetzen« drücken, bedrucken die meisten Drucker anschließend auch das eigentlich falsche Papierformat.

Die Standardoptionen für Papiereinzug und Papiergröße variieren abhängig vom Druckertyp und vom Modell sehr. Sie erreichen diese Einstellungen im Applet GERÄTE UND DRUCKER, wenn Sie das DRUCKEREIGENSCHAFTEN-Dialogfeld des Druckers öffnen, die Registerkarte ALLGEMEIN auswählen und auf die Schaltfläche DRUCKEINSTELLUNGEN klicken. Hier können Sie den Papiereinzug (bei Druckern mit mehreren Papierfächern) und die Papierart festlegen.

Seltsame Abmessungen

Wenn Druckaufträge in merkwürdiger Größe ausgedruckt werden, weist dies üblicherweise darauf hin, dass der Anwender bei deren Einrichtung Fehler gemacht hat. Alle Anwendungen verfügen über Befehle zum Drucken und zur Seiteneinrichtung. Im Rahmen der Seiteneinrichtung oder der Druckeinstellungen können Sie eine Reihe von Druckoptionen festlegen, die sich je nach Einsatz und verwendetem Drucker unterschiedlich auswirken können. Abbildung 26.37 zeigt das Dialogfeld SEITE EINRICHTEN von Word. Bevor Sie dem Drucker die Schuld geben, sollten Sie sich davon überzeugen, dass der Anwender die Seite richtig eingerichtet hat.

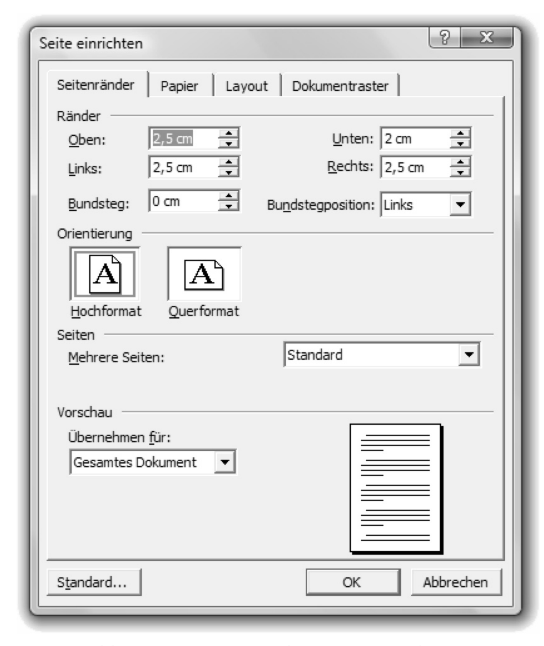


Abb. 26.37: Optionen der Seiteneinrichtung

Wenn Sie wissen, dass die Seite richtig eingerichtet wurde, prüfen Sie noch einmal die Druckertreiber. Deinstallieren Sie die Druckertreiber bei Bedarf und installieren Sie diese neu. Wenn das Problem weiterhin bestehen bleibt, könnte ein ernsthafter Fehler der Druckerelektronik vorliegen. In diesem Fall müssten Sie aber auch ständig Ausdrucke mit denselben seltsamen Abmessungen erhalten, wenn Sie von anderen Anwendungen aus drucken.

Falsch ausgerichtete oder unlesbare Ausdrucke

Wenn Ausdrucke falsch ausgerichtet sind oder zwar drucktechnisch in Ordnung, aber dennoch nicht lesbar sind (z.B. »Hieroglyphen«), weist dies unweigerlich auf beschädigte oder falsche Treiber hin. (Mittlerweile ist es zwar ziemlich schwer, falsche Treiber zu installieren, es lässt sich aber auch nicht ausschließen.) Überzeugen Sie sich davon, dass der richtige Treiber verwendet wird, deinstallieren Sie den Druckertreiber und installieren Sie ihn anschließend neu. Wenn das Problem bestehen bleibt, geben Sie dem Drucker vielleicht einen Auftrag, den dieser gar nicht erfüllen kann. Vielleicht kommunizieren Sie ja über einen PCL-Treiber mit einem PostScript-Drucker. Prüfen Sie noch einmal das Druckermodell, um sich davon zu überzeugen, dass nicht versehentlich die falsche Treibervariante für diesen Drucker installiert worden ist.

Wenn auch das nicht weiterführt, sollten Sie sich vergewissern, dass das Datenkabel in Ordnung ist und dass die Stromversorgung funktioniert. Schließen Sie den Drucker an einer anderen Steckdose an (ohne Überspannungsschutz). Falls der Drucker mehrere Verbindungen unterstützt, sollten Sie eine andere ausprobieren.

Umgang mit Verbrauchsmaterial

Alle Drucker produzieren eine Menge Abfall in Form von Verbrauchsmaterialien. Anschlagdrucker verbrauchen Papier und Farbbänder, Tintenstrahldrucker Papier und Tintenpatronen, Laserdrucker Papier und Tonerkartuschen. Im heutigen umweltbewussten Umfeld wird die Entsorgung der meisten Druckerkomponenten von vielen Gesetzen reguliert. Fragen Sie bei den lokalen Behörden oder dem zuständigen Entsorgungsunternehmen nach, wie die verschiedenen Komponenten zu entsorgen sind, bevor Sie diese wegwerfen. Natürlich sollten Sie Tonerkartuschen nie wegwerfen – manche Unternehmen zahlen sogar für leere Kartuschen!

Wichtig

Bei gefährlichen Komponenten oder Substanzen finden Sie in den Sicherheitsdatenblättern alle notwendigen Informationen zum ordnungsgemäßen Umgang und Anweisungen für den Notfall. Für gewöhnlich werden diese Dokumente an Orten, an denen mit potenziell gefährlichen Stoffen gearbeitet wird, gut sichtbar ausgehängt.

Farben werden falsch ausgedruckt

Wenn Sie farbig drucken, werden früher oder später falsche Farben ausgegeben. Ein erster Schritt ist das Ausdrucken einer entsprechenden Testseite. Auf diese Weise können Sie erkennen, ob das Problem vom Drucker verursacht wird oder dadurch, was und wie Sie drucken.

Fehlerhafte Farben haben manchmal ganz einfache Ursachen, die zunächst überprüft werden sollten. Wenn Sie ein farbiges Dokument ausdrucken, das schwarz-weiß ausgegeben wird, sollten Sie sich vergewissern, dass weder das zum Ausdrucken benutzte Programm noch die Druckereinstellungen für die Verwendung von Graustufen konfiguriert sind. Überprüfen Sie außerdem, ob noch genug farbiger Toner bzw. farbige Tinte vorhanden ist.

Wenn ein eigentlich schwarz-weißer Ausdruck einen seltsamen Farbstich zeigt, könnte es sein, dass der schwarze Toner bzw. die schwarze Tinte zur Neige geht. Scheinbar schwarze Farben sind manchmal aus einer Mischung mit anderen Farben zusammengesetzt. Ist der Schwarzanteil zu gering, kann es zu unerwarteten Farbtönen kommen.

Ist die Farbjustierung des Druckers aus dem Gleichgewicht gekommen, erscheint an den Rändern größerer Objekte möglicherweise ein schmaler farbiger Streifen (für gewöhnlich Zyan, Magenta oder Gelb). Bei Text ist das weniger auffällig – er sieht lediglich etwas verschwommen aus oder wirft scheinbar einen kleinen Schatten. In diesem Fall sollten Sie die Farbjustierung des Druckers kalibrieren.

Überprüfen Sie, ob in den Einstellungen auf Ihrem System und auf dem Drucker selbst irgendwelche Farbanpassungen konfiguriert sind. Ist das der Fall, könnte eine Fehlkonfiguration vorliegen. Wenn der Drucker eine Funktion zur Farbkalibrierung bietet, sollten Sie diese durchführen und prüfen, ob das Problem dadurch behoben wird. Es könnte auch sein, dass Ihr System entweder für den Monitor oder für den Drucker ein falsches Farbprofil verwendet. Im ersten Fall stellt der Drucker die Farben womöglich richtig dar, der Monitor aber nicht. Vergewissern Sie sich, dass auf beiden Geräten kein ungeeignetes Farbprofil zum Einsatz kommt. Wenn die Profile korrekt sind und Ihnen Geräte für eine Farbkalibrierung zur Verfügung stehen, sollten Sie diese nutzen.

Manche Ursachen für fehlerhafte Farbdarstellungen wiegen schwerer. Wenn der Drucker eigene Tonerkartuschen oder Tintenpatronen für die verschiedenen Farben verwendet, wäre es möglich, dass jemand beim Austausch einer Tonerkartusche oder Tintenpatrone die Farben verwechselt hat. Handelt es sich um einen Tintenstrahldrucker, müssen die Röhrchen für den Tintentransport und die Druckköpfe mit erheblichem Zeitaufwand gereinigt werden. Auch wenn wieder die richtigen Farben verwendet werden, kann ein verunreinigter Druckkopf verhindern, dass der Drucker die korrekte Farbe ausgibt. Hier hilft nur eine sorgfältige Reinigung.

Abstürze beim Einschalten

Sowohl Laserdrucker als auch Computer benötigen kurz nach dem Einschalten mehr Energie (der POST beim PC und die Aufwärmphase beim Laserdrucker) als während des normalen Betriebs. Hewlett-Packard empfiehlt, die Reihenfolge beim Einschalten umzukehren. Schalten Sie erst den Laserdrucker ein und warten Sie, bis dessen Aufwärmphase beendet ist, bevor Sie den PC einschalten. Dadurch vermeiden Sie, dass die Geräte das Stromnetz gleichzeitig belasten.

Fehlfunktion der Druckeranzeige

Die kleinen Anzeigen, die bei vielen Druckern und Multifunktionsgeräten eingebaut sind, können Probleme bereiten wie jedes andere Display auch. Das Display kann beispielsweise »einfrieren«, überhaupt nichts anzeigen oder nur eine Farbe anzeigen oder Artefakte aufweisen, wie etwa eine durchgehende Linie, oder einfach nur nach jahrelanger Nutzung verblassen. Leider kann man hier nur wenig tun. Es ist einen Versuch wert, das Gerät aus- und wieder einzuschalten. Manche Hersteller empfehlen, das Gerät einige Minuten komplett vom Stromnetz zu trennen. Funktioniert die Anzeige weiterhin nicht richtig, obwohl das Gerät ansonsten einwandfrei arbeitet und die Probleme nicht unmittelbar nach einer Firmware-Aktualisierung aufgetreten sind, ist es wohl an der Zeit, das Gerät reparieren zu lassen.

26.4.2 Fehlerbehebung bei Matrixdruckern

Matrixdrucker erfordern regelmäßige Wartung, funktionieren aber ewig, wenn Sie diese sorgfältig ausführen. Die Walze, auf der die Drucknadeln auftreffen, und der Druckkopf sollten mit denaturiertem Alkohol sauber gehalten werden. Sorgen Sie auch dafür, dass Zahnräder und Rollen entsprechend den Vorgaben des Herstellers geschmiert werden. Zur Reinigung des Druckkopfs sollten Sie allerdings keine Flüssigkeiten verwenden, da diese dazu führen können, dass das Papier verschmiert und fleckig wird. Vergessen Sie auch nicht, das Farbband regelmäßig zu erneuern.

Die meisten Anschlagdrucker verwenden Papierrollen oder gestapeltes Papier, das kontinuierlich zugeführt wird. Zum Nachfüllen muss also nur die Papierrolle ausgetauscht oder Papier im Papierfach nachgelegt werden. Achten Sie auf eine sorgfältige Ausrichtung der Rolle bzw. des Papierstapels und entfernen Sie gegebenenfalls vorhandene Papierreste. Wie bei anderen Druckern auch kann minderwertiges Papier, Abrieb oder nicht ordnungsgemäß ausgerichtetes Papier zu Papierstaus führen, die Sie beheben können, indem Sie das Papier auf die eine oder andere Art entfernen.

Lesen Sie die Vorgehensweise in der Dokumentation des Druckers nach. Wenn Sie der Anleitung nicht folgen, besteht die Möglichkeit, dass Sie den Drucker beschädigen. Häufig gibt es einen manuellen Papiervorschub oder Sie müssen in einer bestimmten Richtung an einem festsitzenden Blatt Papier ziehen. Das Transportsystem kann Schaden nehmen, wenn man hierbei nicht ordnungsgemäß vorgeht.

Unansehnlicher Text

Weiße, horizontale Streifen, die durch den Text verlaufen, weisen auf einen verschmutzten oder beschädigten Druckkopf hin. Versuchen Sie, den Druckkopf mit ein wenig denaturiertem Alkohol zu säubern. Wenn das Problem weiterhin besteht, ersetzen Sie den Druckkopf. Beim Druckerhersteller oder bei Drittanbietern sind Druckköpfe für die meisten Drucker kurzfristig lieferbar. Wenn die Zeichen oben oder unten abgeschnitten werden, muss der Druckkopf wahrscheinlich neu justiert werden. Einzelheiten dazu entnehmen Sie den Anleitungen des Herstellers. Werden die Zeichen im Laufe der Zeit zunehmend blasser, ist der Druckkopf verschlissen; ersetzen Sie ihn.

Unansehnliche Seiten

Wenn das Papier mit kleinen Punkten übersät und verschmiert ist, dann ist die Andruckwalze verschmutzt. Säubern Sie sie mit denaturiertem Alkohol. Wenn das Schriftbild blass wirkt, das Farbband aber noch in Ordnung ist, justieren Sie den Druckkopf neu, damit er sich dichter an der Walze befindet. Wenn das Druckbild auf der einen Seite des Blattes zwar einwandfrei ist, zur anderen Seite hin aber schwächer wird, dann ist die Walze dejustiert. Die Andruckwalzen lassen sich im Allgemeinen nur schwer neu justieren, sodass es meist angeraten ist, den Drucker zur Wartung dem Hersteller zu überlassen.

26.4.3 Fehlerbehebung bei Thermodruckern

Im Vergleich zu anderen Druckertypen sind Thermodrucker einfach zu warten und auch die Fehlerbehebung bereitet nur wenig Probleme. Bei Thermodirektdruckern müssen Sie sich nur um drei Dinge kümmern: das Heizelement, die Walzen und das Papier. Bei Thermowachsdruckern kommen noch die Thermowachsbänder hinzu.

Zur Reinigung des Heizstabs müssen Sie den Drucker ausschalten und gemäß der Herstelleranleitung öffnen. Verwenden Sie denaturierten Alkohol und ein fusselfreies Tuch, um das Heizelement abzuwischen. Dabei müssen Sie ein wenig Druck anwenden, um eine gründliche Reinigung zu erzielen. Säubern Sie die Walzen ebenfalls mit einem Tuch oder mit Druckluftspray. Achten Sie darauf, dass sich keine Papierrückstände auf den Walzen befinden, damit der Papiertransport reibungslos vonstattengeht. Zum Austausch der Papierrolle muss lediglich die leere Rolle entfernt und durch eine neue ersetzt werden. Übersehen Sie dabei aber nicht, das Papier durch das Heizelement hindurchzuführen, da der Druck sonst natürlich nicht funktioniert. Das Ersetzen des Thermowachsbands ist ähnlich einfach wie das der Papierrolle. Achten Sie auch hier auf die korrekte Führung des Bandes durch das Heizelement. Falls es bei der Installation des Bandes irgendwelche Besonderheiten gibt, ist dies der Dokumentation des Herstellers zu entnehmen.

26.4.4 Fehlerbehebung bei Tintenstrahldruckern

Tintenstrahldrucker sind zuverlässige Geräte, die nur sehr wenig Wartung erfordern, sofern sie innerhalb des vorgesehenen Rahmens genutzt werden. (Intensiv genutzte Geräte erfordern mehr Wartung.) Aufgrund der niedrigen Preise der Geräte wissen die Hersteller, dass deren Besitzer nicht bereit sind, viel Geld für die Wartung auszugeben. Wenn Sie nur die einfachsten Wartungsaufgaben ausführen, dann halten die Drucker meist problemlos viele Jahre lang. Tintenstrahler enthalten meist eingebaute Wartungsprogramme, die Sie von Zeit zu Zeit ausführen sollten, um das Gerät in gutem Betriebszustand zu halten.

Wartung von Tintenstrahldruckern

Tintenstrahldrucker verschmutzen weit weniger stark als Laserdrucker und die meisten Hersteller empfehlen keine periodische Reinigung. Sofern dies vom Hersteller nicht ausdrücklich empfohlen wird, sollten Sie Tintenstrahler nicht mit einem Staubsauger reinigen. Tintenstrahler werden zwar meist ohne Wartungskits geliefert, enthalten dafür aber zumeist umfassende Wartungsprogramme (Abbildung 26.38). Üblicherweise besteht das größte Problem darin, die entsprechenden Programme zu finden. Halten Sie nach einer entsprechenden Option bei den Druckereigenschaften, einer Option im Startmenü oder einem Symbol auf dem Desktop Ausschau. Irgendwo gibt es dieses Programm!



Abb. 26.38: Wartungsprogramm eines Tintenstrahldruckers

Wenn Sie einen Tintenstrahler erstmals einrichten, dann werden Sie oft aufgefordert, Programme zur korrekten Ausrichtung der Druckköpfe auszuführen. Dabei drucken Sie eine Testseite aus, die dann auf den Scanner gelegt werden muss (sofern vorhanden), oder Sie wählen in einem Menü aus, welche der ausgedruckten nummerierten Zeilen am besten ausgerichtet sind.

Wenn diese Programme nicht ausgeführt werden, dann erkennen Sie dies an der Druckqualität. Die Prozedur kann aber jederzeit und beliebig oft ausgeführt werden. Wenn ein Drucker transportiert wird, auf den Boden gefallen ist oder einfach eine Zeit lang unbeaufsichtigt gearbeitet hat, dann lohnt es sich häufig, die Prozedur zur Ausrichtung der Druckköpfe erneut auszuführen. Manche Drucker führen sie hin und wieder sogar automatisch durch.

Tintenpatronen lassen sich normalerweise leicht ersetzen. Der genaue Ablauf kann sich von Drucker zu Drucker jedoch stark unterscheiden. Lesen Sie in der Dokumentation nach. Normalerweise klappt man den Drucker auf, um den Druckkopf freizulegen, an dem eine oder mehrere Tintenpatronen befestigt sind. Falls der Druckkopf nicht zugänglich ist, dürfen Sie nicht versuchen, ihn mit Gewalt zu bewegen. Bei vielen Druckern wird der Druckkopf in die Mitte bewegt, damit er gut zugänglich ist. Dazu muss das Gerät jedoch eingeschaltet werden, bevor Sie die Tintenpatronen wechseln können.

Die Tintenpatronen rasten meist einfach ein, bei manchen Druckern gibt es jedoch auch Halteklammern. Suchen Sie auf dem Druckkopf oder den Halteklammern nach Hinweisen, welche Tintenpatrone wohin gehört. Folgen Sie beim Entfernen der zu tauschenden Tintenpatrone den Anweisungen

des Herstellers und entnehmen Sie die neue Patrone der Verpackung. Suchen Sie nach einem kleinen Klebeband oder einem anderen Schutz, der die Kontakte und/oder die Düsen abdeckt. Vergewissern Sie sich, dass Sie beim Einsetzen der Patrone der Anleitung sorgfältig folgen, denn eine nicht richtig sitzende Tintenpatrone könnte mit anderen Bauteilen kollidieren, wenn sich der Druckkopf bewegt. Nach dem Einsetzen der Patrone und Zuklappen des Druckers sollte der Druckkopf zu seiner Standardposition bewegt werden.

Probleme von Tintenstrahldruckern

Habe ich behauptet, dass Sie Tintenstrahler nie reinigen sollten? Nun, das mag ja für den Drucker selbst zutreffen, aber es gibt einen Teil des Druckers, der von gelegentlicher Reinigung profitiert: die Düsen des Druckkopfs eines Tintenstrahlers. Die Düsen sind die winzigen Röhrchen, mit denen die Tinte auf das Papier geschossen wird. Ein verbreitetes Problem bei Tintenstrahldruckern ist das Eintrocknen der Düsen nach bereits relativ kurzer Zeit der Nichtbenutzung, sodass keine Tinte mehr austreten kann. Wenn der Drucker Windows zwar mitteilt, dass er druckt und auch Papier auswirft, aber nichts auf dem Papier erscheint (das geschieht meist dann, wenn Sie nur schwarzen Text drucken) oder nur bestimmte Farben gedruckt werden, dann liegt es sehr wahrscheinlich daran, dass die Tinte eingetrocknet ist und die Düsen verstopft hat.

Hinweis

Die von Tintenstrahlern verwendeten Tinten sind wasserlöslich. Daher ist zur Reinigung der Düsen Wasser besser geeignet als Alkohol.

Das Verfahren zur Reinigung der Druckköpfe sieht bei jedem Tintenstrahler etwas anders aus. Bei älteren Geräten müssen Sie üblicherweise bestimmte Tasten am Drucker betätigen, um das Wartungsprogramm zu starten. Bei moderneren Tintenstrahlern können Sie auf die Wartungsprogramme zur Reinigung der Druckköpfe (auch) von Windows aus zugreifen.

Hinweis

Manchmal ist es notwendig, die Druckköpfe eines Tintenstrahldruckers zu reinigen, aber ich empfehle nicht, dies regelmäßig vorbeugend zu tun. Bei der Reinigung wird eine Menge der sehr teuren Tinte verbraucht, deshalb sollten Sie dies nur dann ausführen, wenn ein Druckproblem auf einen verstopften oder verschmutzten Druckkopf hinweist.

Verwenden Sie den Tintenstrahldrucker regelmäßig – das ist die beste Wartung. Wenn die Düsen von Tinte durchflossen werden, verhindert das, dass sie austrocknen und verstopfen. Und wenn Sie eine Woche lang nichts ausdrucken müssen, geben Sie einfach eine Testseite aus.

Ein weiteres Problem, das zuweilen auftritt, ist der ärgerliche Einzug mehrerer Blätter gleichzeitig. Meist handelt es sich dabei eigentlich nicht um ein Problem des Druckers selbst. Feuchtigkeit kann dafür sorgen, dass die Blätter aneinanderkleben. Manchmal ist aber auch ein überhitzter Drucker der Schuldige. Wenn Sie also pausenlos viele Dokumente ausdrucken, dann sollten Sie dem Drucker besser hie und da eine Kaffeepause gewähren. Achten Sie auch darauf, dass Sie das Papier vor dem Einlegen in den Papierschacht auffächern, um die Blätter voneinander zu trennen.

Schließlich befindet sich im Wartungsbereich des Druckers, in dem die Druckköpfe geparkt werden, üblicherweise ein kleiner Behälter oder Tank, der die überschüssige Tinte beim Reinigungsprozess auffängt. Wenn der Drucker über einen solchen Auffangbehälter verfügt, prüfen Sie, wie voll er ist. Wenn der Behälter überläuft und die Tinte auf die Platine oder sogar auf das Netzteil des Druckers tropft, dann führt dies zur Beschädigung des Druckers. Wenn der Behälter bereits reichlich voll ist, dann können Sie überschüssige Tinte mit einem zusammengedrehten Papiertaschentuch aufsaugen. Dabei sollten Sie besser Latex- oder Kunststoffhandschuhe tragen. Beseitigen Sie verschüttete Tinte mit einem feuchten Papiertaschentuch.

26.4.5 Fehlerbehebung bei Laserdruckern

Es gibt einige Probleme, die bei Laserdruckern auftreten können. Bevor wir uns aber damit befassen, werden wir uns erst einmal ein paar vorbeugende Maßnahmen ansehen, mit denen derartige Probleme *vermieden* werden können.

Vorsicht

Vor Wartungsarbeiten an einem Laserdrucker sollten Sie diesen *immer* abschalten und von der Stromversorgung trennen! Setzen Sie sich nicht den gefährlich hohen Spannungen aus, die in diesen Geräten vorhanden sein können.

Wartung von Laserdruckern

Anders als beim PC folgt die Wartung und Fehlersuche bei Laserdruckern einem recht einheitlichen und bewährten Verfahren. Befolgen Sie diese Schritte, damit der Drucker lange in gutem Zustand und einsatzfähig bleibt.

Reinigung Laserdrucker sind in der Regel recht robust konstruiert. Eine sorgfältige Reinigung bei jedem Austausch der Tonerkartusche kann jedoch dessen Leben verlängern, wodurch er jahrelang hält. Ich kenne viele Beispiele für HP-LaserJets, die auch nach mehr als einem Dutzend Betriebsjahren noch einwandfrei funktionieren. Derart lange Einsatzzeiten lassen sich aber wohl nur erreichen, wenn die Drucker tadellos sauber gehalten werden.

Im Allgemeinen gibt es nur zwei Ursachen für die Verschmutzung eines Laserdruckers. Die erste Ursache bilden überschüssige Tonermengen. Der Toner verteilt sich langsam im ganzen Drucker. Die zweite Ursache ist Papierstaub. Dieser lagert sich vorwiegend an jenen Stellen im Drucker ab, an denen das Papier über Walzen geführt wird oder die Mechanik das Papier aufnimmt. Anders als (schwarzer) Toner lässt sich Papierstaub gut erkennen und kann als Hinweis darauf dienen, dass der Drucker einer Reinigung bedarf. Nicht nur bei Druckern ist es üblicherweise am besten, wenn man Rückstände mit einer Dose Druckluft aus dem Gehäuse bläst. Das sollte möglichst außerhalb geschlossener Räume erledigt werden, wenn man hinterher nicht wie ein Schornsteinfeger aussehen will! Wenn Sie den Drucker innerhalb geschlossener Räume reinigen müssen, sollten Sie dazu Staubsauger verwenden, die speziell für die Reinigung elektronischer Komponenten entwickelt worden sind, wie die Geräte von Metro Vacuum.

Für alle Laserdrucker gibt es spezielle Reinigungsverfahren. Ein Bereich wird bei den Reinigungsanleitungen der meisten Laserdrucker aber vergessen. In allen Laserdruckern gibt es eine Reihe von Gummi-Führungsrollen, über die das Papier beim Druckvorgang geleitet wird. Diese kleinen Rollen nehmen mit der Zeit leicht Schmutz und Papierstaub auf, wodurch sie rutschig werden und Papierstaus verursachen können. Diese Rollen lassen sich aber einfach mit ein wenig 90-prozentigem Alkohol und einem fusselfreien Lappen reinigen. Der Alkohol entfernt die Rückstände und Gummiabrieb. Sie können die Rollen und Trennelemente aber auch aufrauen, damit sie ihre Aufgabe wieder besser erfüllen, indem Sie diese mit ein wenig Alkohol befeuchten und mit einem Topfreiniger (nicht aus Metall!) bearbeiten.

Vorsicht

Die Belichtungstrommel, die sich üblicherweise (aber nicht immer) in der Tonerkartusche befindet, lässt sich bei Verschmutzung abwischen. *Lassen Sie dabei äußerste Vorsicht walten!* Wenn die Trommel verkratzt wird, finden Sie diese Kratzer anschließend auf allen ausgedruckten Seiten wieder. Dann hilft nur noch ein Austausch der kompletten Tonerkartusche oder Belichtungstrommel.

Wenn Sie genau nach Vorschrift vorgehen wollen, dann besorgen Sie sich das Wartungshandbuch des Druckers. Leider erhalten Sie diese Handbücher nicht von allen Herstellern. Vielfach können Sie die

wichtigsten Einzelheiten auch der Schnellanleitung entnehmen, die außerdem bei der Fehlersuche gute Dienste leistet!

Regelmäßige Wartung Damit der Drucker problemlos seine Arbeit verrichtet, muss er nicht nur sauber gehalten werden. Wann und welche Komponenten in regelmäßigen Zeitabständen ausgewechselt werden müssen, erfahren Sie am besten vom Druckerhersteller. Wenn Sie den Angaben des Herstellers folgen, trägt das dazu bei, dass der Drucker über Jahre hinweg problemlos und zuverlässig funktioniert.

Viele Hersteller bieten Wartungskits mit Komponenten an, die regelmäßig getauscht werden sollten. Diese Wartungskits enthalten häufig eine Fixiereinheit und eine oder mehrere Rollen und weiteres Zubehör. Üblicherweise müssen Sie nach der Installation eines Wartungskits einen Seitenzähler zurücksetzen, damit der Drucker nach einer bestimmten Anzahl von Ausdrucken darauf hinweisen kann, wann die Wartungsarbeiten wieder fällig sind.

Einige Ozonfilter lassen sich mit einem Staubsauger reinigen, andere werden einfach ausgetauscht. Folgen Sie den Empfehlungen des Herstellers. Die Fixiereinheit kann mit 90-prozentigem denaturiertem Alkohol gereinigt werden. Prüfen Sie, ob die (mit Teflon beschichteten) beheizten Rollen Grübchen oder Kratzer aufweisen. Wenn ihre Oberfläche beschädigt sein sollte, dann tauschen Sie die Fixiereinheit aus.

Die meisten Drucker geben eine Fehlermeldung aus, wenn die Fixiereinheit beschädigt ist oder zu heiß wird und ersetzt werden muss. Andere geben eine vorbeugende Warnmeldung bzw. einen Fehlercode aus, wenn eine bestimmte Anzahl von Seiten gedruckt wurde. Folgen Sie auch hier wieder den Empfehlungen des Herstellers.

Hinweis

Sollte die Thermosicherung (die dafür sorgt, dass die Fixiereinheit nicht überhitzt) ausfallen, dann kann ein Austausch der Fixiereinheit erforderlich sein. Einige Geräte enthalten mehr als eine Thermosicherung. Auch hier sollten Sie den Empfehlungen des Herstellers folgen. Viele Hersteller bieten Kits an, die Sie nach einer bestimmten Anzahl gedruckter Seiten warnen und darauf hinweisen, wenn Sie die Fixiereinheit und die Rollen und Führungen auswechseln sollten.

Der untere Koronadraht kann mit 90-prozentigem, denaturiertem Alkohol auf einem Baumwolllappen gereinigt werden. Wenn der Draht beschädigt ist, dann können Sie ihn ersetzen. Vielfach rastet er einfach ein oder wird von ein paar Schrauben an Ort und Stelle gehalten. Papierführungen lassen sich auch mit einem alkoholgetränkten Lappen reinigen.

Vorsicht

Lassen Sie die Fixiereinheit vor der Reinigung immer erst abkühlen, da sie 100 bis 150 Grad Celsius heiß werden kann!

Manche Laserdrucker bieten – wie Tintenstrahldrucker – die Möglichkeit einer Farbkalibrierung, um die Qualität von farbigen Ausdrucken zu gewährleisten. Dadurch wird sichergestellt, dass Farben an der richtigen Position und in der richtigen Menge ausgegeben werden. Manche Geräte führen eine solche Kalibrierung hin und wieder automatisch durch. Ansonsten können Sie dem Handbuch oder bei manchen Druckern auch der Anzeige des Geräts entnehmen, wann eine Kalibrierung angebracht ist und wie sie durchgeführt wird.

Probleme bei Laserdruckern

Probleme bei Laserdruckern lassen sich üblicherweise an der mangelhaften Druckqualität erkennen. Einer der wichtigsten Tests für alle Drucker ist der Ausdruck allgemeiner oder spezifischer *Druckertest-*

seiten. Dazu hält man üblicherweise einen Taster beim Start des Druckers gedrückt oder nutzt die mit dem Drucker gelieferten Wartungsprogramme.

Blasser Ausdruck oder leere Seiten Wenn sehr blasse oder sogar leere Seiten ausgegeben werden, weist das üblicherweise darauf hin, dass der Toner ausgegangen ist. Wenn der Drucker noch Toner hat, aber dennoch nichts ausgedruckt wird, sollten Sie den Ausdruck einer Testseite versuchen. Wenn diese ebenfalls leer ist, entfernen Sie die Tonerkartusche und werfen einen Blick auf die Bildtrommel. Wenn darauf noch das Druckbild zu sehen ist, dann wissen Sie, dass der untere Koronadraht oder das Hochspannungsnetzteil defekt ist. Aus dem Wartungshandbuch des Druckers können Sie erfahren, wie Sie die tatsächliche Ursache ermitteln und die betroffenen Bauteile austauschen können.

Verschmutzte oder verwischte Ausdrucke Wenn der Fixiermechanismus in einem Laserdrucker allmählich verschmutzt, dann bleibt ein wenig Tonerstaub auf dem ganzen Blatt und insbesondere auf dessen Rückseite zurück. Wenn Sie auf den Ausdrucken Tonerflecken feststellen, sollten Sie den Drucker reinigen.

Wenn Ausdrucke verschmiert sind oder sich Toner vom Blatt ablöst, wenn Sie mit dem Finger darüber streichen, dann arbeitet die Fixiereinheit vermutlich nicht korrekt. Die zur Fixierung erforderliche Temperatur hängt auch von der Papierart ab. Funktioniert die Fixierung nicht, sollten Sie testweise eine leichtere Papiersorte verwenden. Unter Umständen muss die Fixiereinheit ersetzt werden.

Geisterbilder Auf der gedruckten Seite erscheinen manchmal in regelmäßigen Abständen Geisterbilder. Das kann daran liegen, dass die Bildtrommel nicht vollständig entladen wurde (und Toner für eines der vorherigen Bilder anzieht), daran, dass ein vorheriges Bild derart viel Toner benötigt hat, dass die Versorgung mit geladenem Toner nicht mehr ausreicht, oder daran, dass der Toner nicht hinreichend geladen wurde. Manchmal wird dieser Effekt auch von einer verschlissenen Reinigungsrakel verursacht, die den Toner nicht mehr richtig von der Trommel entfernen kann.

Helle und dunkle Geisterbilder Eine ganze Reihe von Problemen können sowohl helle als auch dunkle Geisterbilder verursachen. Die häufigste Ursache heller Geisterbilder ist aber das Nachlassen der Entwicklereinheit. Wenn Laserdrucker äußerst dunkle oder komplexe Seiten drucken sollen, können sie derart viel Toner verbrauchen, dass für die nachfolgende Seite nicht genügend Toner zur Verfügung steht. Sie können den Tonerverbrauch und damit die Wahrscheinlichkeit des Entstehens von Geisterbildern durch die folgenden Maßnahmen verringern:

- Verringerung der Druckauflösung (300 statt 600 dpi)
- Andere Muster verwenden
- Vermeidung von 50-Prozent-Grauwerten, bei denen die einzelnen Dots abwechselnd gedruckt bzw. nicht gedruckt werden
- Änderung des Seitenlayouts, sodass Graustufenmuster nicht auf schwarze Bereiche folgen
- Aufhellen dunkler Bereiche und Abdunkeln heller Bereiche
- Ausdruck im Querformat
- Einstellung der Druckdichte und des Kantenglättungsverfahrens (RET)
- Druck einer komplett leeren Seite direkt vor der Seite mit dem Geisterbild innerhalb desselben Druckauftrags

Darüber hinaus können niedrige Temperaturen und zu geringe Luftfeuchtigkeit Probleme mit Geisterbildern fördern. Angaben für die Umgebungsbedingungen finden Sie im Benutzerhandbuch des Druckers. Dunkle Geisterbilder werden manchmal von einer beschädigten Trommel verursacht. Dann lässt sich das Problem möglicherweise durch Austausch der Tonerkartusche beheben. Helle Geisterbilder lassen sich auf diese Weise *nicht* beseitigen. Der Austausch anderer Komponenten hat üblicherweise keinen Einfluss auf Probleme mit Geisterbildern, da es sich dabei um einen Nebeneffekt des gesamten Druckprozesses handelt.

Senkrechte weiße Linien Das Auftreten senkrechter weißer Linien weist für gewöhnlich auf Verklumpungen des Tonerpulvers hin, sodass dieses nicht wirklich gleichmäßig auf die Trommel aufgetragen werden kann. Schütteln Sie die Tonerkartusche, um Klumpen aufzulösen bzw. zu verlagern. Wenn das nicht hilft, sollten Sie die Tonerkartusche ersetzen.

Fleckige Ausdrucke Dies liegt meist an einer ungleichmäßigen Verteilung des Toners, die besonders häufig auftritt, wenn der Toner langsam zur Neige geht. Schütteln Sie die Tonerkartusche seitlich hin und her und versuchen Sie den Ausdruck dann erneut. Sorgen Sie auch dafür, dass der Drucker waagerecht steht. Schließlich sollten Sie sich noch davon überzeugen, dass das Papier nicht stellenweise feucht geworden ist. Wenn die Flecken regelmäßig angeordnet sind, sollten Sie prüfen, ob sich Fremdobjekte auf den Fixierwalzen oder der Trommel befinden.

Regelmäßig angeordnete Flecken Wenn die Flecken in regelmäßigen Abständen auftreten, könnte die Trommel beschädigt sein, oder es könnte ein wenig Toner an den Fixierwalzen hängen geblieben sein. Wischen Sie die Fixierwalzen ab und prüfen Sie, ob die Trommel Beschädigungen aufweist. Wenn die Trommel beschädigt sein sollte, tauschen Sie sie aus.

Reliefeffekt Wenn die Ausdrucke einen Reliefeffekt aufweisen (ähnlich dem Nachzeichnen einer Münze unter einem Blatt Papier mit einem Bleistift), befindet sich fast immer ein Fremdobjekt auf einer Walze. Reinigen Sie die Walzen z.B. mit 90-prozentigem, denaturiertem Alkohol oder einem leicht mit Wasser befeuchteten, weichen Lappen, um das Fremdobjekt zu entfernen. Wenn sich das Fremdobjekt auf der lichtempfindlichen Trommel befindet, müssen Sie wahrscheinlich die Tonerkartusche austauschen. Ein Reliefeffekt kann auch entstehen, wenn die Kontrasteinstellung zu hoch gewählt wurde. Bei der Kontrasteinstellung handelt es sich um einen Regler im Innern des Gerätes (bei älteren Modellen manchmal auch von außen zugänglich). Werfen Sie einen Blick in das Handbuch und stellen Sie fest, ob es einen solchen Regler beim betroffenen Drucker gibt und wo sich dieser befindet.

Unvollständige Zeichen Probleme mit unvollständig gedruckten Zeichen auf Transparentfolien lassen sich manchmal dadurch beheben, dass die Druckdichte erhöht wird. Zudem sollten Sie sich von der Qualität der eingesetzten Kunststoffmaterialien überzeugen und ausschließlich Folien verwenden, die ausdrücklich für den Einsatz in Laserdruckern geeignet sind.

Zerknitterte Seiten In Laserdruckern gibt es bis zu vier Walzen. Neben den Heiz- und Andruckwalzen der Fixiereinheit transportieren weitere Walzen die Blätter auf ihrem Weg von der Papierzufuhr bis in den Auswurfschacht. Diese Walzen biegen das Papier so, dass es normalerweise glatt durch den Drucker transportiert und nicht zerknittert wird, weshalb im Normalfall kein Papierstau im Drucker auftreten kann. Wenn das Papier sichtbar zerknittert wird, sollten Sie eine andere Papiersorte ausprobieren. Bestimmte Papiersorten (z.B. solche, die Baumwollfasern enthalten) knittern leichter als andere. Sie können die Ausgabe auch in den Auswurfschacht für Einzelblätter umleiten und so eine Transportwalze umgehen. (Dies empfiehlt sich bei dickeren Papiersorten oder Karton ohnehin.) Für dieses Problem gibt es keine Hardwarelösung, da es sich einfach um einen Nebeneffekt des Druckprozesses handelt.

Papierstau In allen Druckern kann es gelegentlich zum Papierstau kommen. Wenn sich das Papier staut, folgen Sie zunächst den Angaben des Herstellers für derartige Problemfälle. Manche Drucker können allzu leicht beschädigt werden, wenn Sie das gestaute Papier einfach herausziehen! Wenn der Drucker zwar einen Papierstau meldet, sich darin aber kein Papier befindet, dann liegt sehr wahrscheinlich ein Problem mit einem der vielen Papierstau-Sensoren im Innern des Druckers vor. Dann ist es an der Zeit, den Drucker in die Werkstatt zu bringen.

Einzug mehrerer Blätter Wenn der Drucker mehrere Blätter gleichzeitig greift, versuchen Sie es zunächst mit einem neuen Stapel Papier, den Sie in die Papierkassette einlegen. Wenn das funktioniert, dann handelt es sich wahrscheinlich um ein Feuchtigkeitsproblem. Wenn dies nicht hilft, dann prüfen Sie die Trennvorrichtung am Drucker. Dabei handelt es sich um ein kleines Kork- oder Gummiteilchen, das die Blätter voneinander trennt, wenn sie aus der Papierkassette gezogen werden. Verschlissene Trennvorrichtungen sind oft blank oder sehen buchstäblich verschlissen aus. Meist kann die Trennvorrichtung leicht ersetzt werden.

Papiereinzug funktioniert nicht Wenn sich im Papierfach des Druckers Papier befindet, dieses beim Drucken jedoch nicht eingezogen wird, müssen Sie Andruckrollen des Papiereinzugs reinigen (oder sogar ersetzen). Vergewissern Sie sich auch, dass der Drucker so eingestellt ist, dass er tatsächlich das fragliche Papierfach verwendet. Überprüfen Sie auch das Papier. Ist das Papierfach womöglich zu voll? Ist das Papier richtig ausgerichtet? Ist es vielleicht gewellt oder geknickt? Ist das Gewicht und die

Beschichtung des Papiers die übliche? Ist in den Druckereinstellungen die richtige Papiersorte konfiguriert? Wenn Sie eine andere Papiersorte verwenden, sollten Sie testen, ob das sonst verwendete Papier korrekt eingezogen wird. Wenn das Papierfach verstellbare Papierführungen besitzt, sollten Sie überprüfen, ob sie das Papier vielleicht zu sehr festhalten.

Verzerrte, überdruckte oder verformte Zeichen Schlecht ausgebildete Zeichen können sowohl auf ein Problem mit dem Papier (bzw. den Druckmedien) als auch auf ein Problem der Hardware hinweisen.

Falsche Druckmedien können zu einer ganzen Reihe derartiger Probleme führen. Vermeiden Sie zu raue oder zu glatte Papiersorten. Zu raues Papier kann den Fixiervorgang behindern. Wenn das Papier zu glatt ist (wie z.B. einige beschichtete Papiersorten), kann es zu Störungen des Papiertransports kommen, die zu unsauberen oder überschriebenen Zeichen führen. Auch wenn es spezielle Papiersorten für Laserdrucker gibt, kommen alle Laserdrucker mit normalem Fotokopierpapier gut zurecht. Sorgen Sie dafür, dass das Papier nicht zu viel Feuchtigkeit aufnimmt. Öffnen Sie daher die Papierpakete erst, wenn Papier in die Kassette eingelegt werden soll. Fächern Sie das Papier immer erst auf, bevor Sie es in die Kassette legen, speziell wenn es bereits eine Zeit lang außerhalb der Verpackung aufbewahrt worden ist.

Aufgrund der Haltbarkeit gut gewarteter Laserdrucker verursacht die Hardware zwar eher selten Druckprobleme, kann aber hie und da doch einmal versagen. Glücklicherweise lässt sich die Hardware recht leicht prüfen. Die meisten Laserdrucker verfügen über Selbsttestfunktionen, die mit einem entsprechenden Ausdruck kombiniert sind oder zumindest separate Testdruckmöglichkeiten bieten. Dieser Selbsttest zeigt, ob der Laserdrucker Seiten korrekt ausgeben kann, ohne Druckbefehle vom Rechner zu empfangen. Über den Selbsttest lässt sich die Frage, ob der Drucker oder der Rechner den Fehler verursacht, recht leicht klären. Starten Sie den Selbsttest, wenn es um die Ermittlung der Ursache von Verbindungs- und Konfigurationsproblemen geht.

Zu den möglichen Lösungen zählt das Auswechseln der Tonerkartusche, gerade wenn sich sonderbare Geräusche vernehmen lassen. Dann sollten Sie die Kabelverbindungen prüfen und das Datenkabel ersetzen, insbesondere wenn Knicke oder Beschädigungen sichtbar sind oder Gegenstände auf dem Kabel stehen oder gestanden haben. Wenn der Drucker über ein Bedienfeld verfügt, können Sie die anspruchsvolleren Funktionen und höhere Geschwindigkeiten abschalten, um festzustellen, ob diese nicht funktionieren oder von der aktuellen Softwarekonfiguration nicht unterstützt werden (Einzelheiten zur Konfiguration können Sie den Handbüchern entnehmen). Wenn diese Lösungen nicht funktionieren, könnte es sein, dass sich das Problem nicht vom Anwender beheben lässt. Nehmen Sie Kontakt zu einem autorisierten Reparaturdienst auf.

26.4.6 Fehlerbehebung bei 3-D-Druckern

Das Erstellen von Objekten durch das Schmelzen und Verformen von Kunststoff hat das Potenzial, ein ziemliches Chaos zu verursachen. Zu den typischen Problemen gehören ungewollte Kunststofffäden, die verschiedene Hohlräume miteinander verbinden, Überhitzungen, die einen Teil des Druckergebnisses wieder einschmelzen, oder verschobene Schichten, die dann nicht mehr richtig ausgerichtet sind. Die verschiedenen Kunstofffilamente sind von unterschiedlicher Qualität, was den ohnehin schon komplexen Vorgang nicht gerade vereinfacht. Auf den ersten Blick spart die Verwendung von Filamenten geringer Qualität natürlich Geld, aber sie kann schnell zu einer Verstopfung des Extruders führen.

3-D-Drucker gibt es zwar schon seit rund zehn Jahren, die Technologie bereitet aber noch immer beträchtliche Schwierigkeiten. Die Fehlerbehebung bei 3-D-Druckern geht weit über den Rahmen der CompTIA A+-Prüfung hinaus, vor allem, weil sich die Vorgänge bei der Vielzahl von Druckermodellen so immens voneinander unterscheiden. In der Regel sollten Sie auf der Website des Herstellers nach Hilfe suchen. Oder besuchen Sie eine der vielen ausgezeichneten von Enthusiasten betriebenen Websites, wie etwa `http://www.fabbaloo.com`.

26.5 Wiederholung

26.5.1 Fragen

1. Mit welchem Verfahren bringen die meisten Tintenstrahldrucker die Tinte zu Papier?
   A. Elektrostatische Entladungen
   B. Schwerkraft
   C. Luftdruck
   D. Elektrisch leitende Plättchen
2. Was erzeugt bei einem Laserdrucker das Bild auf der Belichtungstrommel?
   A. Koronadraht
   B. Laser-Belichtungseinheit
   C. Unterer Koronadraht
   D. Toner
3. Was ist die korrekte Reihenfolge der Vorgänge beim Laserdruck?
   A. Verarbeiten, Reinigen, Laden, Belichten, Entwickeln, Übertragen, Fixieren
   B. Verarbeiten, Laden, Belichten, Entwickeln, Übertragen, Fixieren, Reinigen
   C. Reinigen, Belichten, Entwickeln, Übertragen, Verarbeiten, Fixieren, Laden
   D. Reinigen, Laden, Belichten, Verarbeiten, Entwickeln, Fixieren, Übertragen
4. Was schlägt bei einem Matrixdrucker zur Erzeugung des Druckbildes physisch gegen das Farbband?
   A. Elektromagneten
   B. Drucknadeln
   C. Typenrad
   D. Drucktypen
5. Bei welchen der folgenden Objekte handelt es sich bei Matrixdruckern um Verbrauchsmaterialien? (Wählen Sie zwei Antworten aus.)
   A. Antriebsmotor
   B. Papier
   C. Schwungrad
   D. Farbband
6. Was muss in regelmäßigen Zeitabständen mit einem Staubsauger gereinigt oder ersetzt werden, um durch die Aktivität des Koronadrahts verursachte Schäden zu vermeiden?
   A. Die Gummiwalzen
   B. Der Ozonfilter
   C. Der Transferfilter
   D. Die Reinigungsrakel
7. Welche der folgenden Schnittstellen wird von den meisten Druckern unterstützt?
   A. PS/2
   B. USB
   C. Infrarot
   D. RS-232

8. Bei einem Einzelplatzdrucker ist der Ausdruck der Testseite zwar in Ordnung, anschließend sehen Ihre endgültigen Ausdrucke aber mehr als bescheiden aus. Wo ist der Fehler wahrscheinlich zu suchen?
   A. Der Toner geht zur Neige.
   B. Ein Fehler der Fixiereinheit
   C. Die Druckerschnittstelle
   D. Fehlerhafte Softwarekonfiguration
9. Welcher Druckprozess verwendet wärmeempfindliche Kunststoffbänder, in die verschiedene Farben eingebettet sind?
   A. Farbsublimation
   B. Tintenstrahl
   C. Tintendispersion
   D. Farbdispersion
10. Mit welchem Werkzeug können Sie feststellen, warum ein Druckauftrag nicht gedruckt wurde?
   A. Druckertreiber
   B. Druckereinrichtung
   C. Druckerwarteschlange
   D. Systemeinrichtung

26.5.2 Antworten

1. **D.** Bei den meisten Tintenstrahldruckern werden elektrisch leitende Plättchen benutzt, um die Tinte auf das Papier zu bringen.
2. **B.** Die Laserbelichtungseinheit erzeugt ein Bild auf der Belichtungstrommel.
3. **B.** Verarbeiten, Laden, Belichten, Entwickeln, Übertragen, Fixieren und Reinigen ist die richtige Reihenfolge der Vorgänge.
4. **B.** Die Drucknadeln schlagen bei Matrixdruckern physisch gegen das Farbband.
5. **B, D.** Papier und Farbbänder zählen bei Matrixdruckern zu den Verbrauchsmaterialien.
6. **B.** Der Ozonfilter sollte regelmäßig mit einem Staubsauger gereinigt oder ausgewechselt werden.
7. **B.** Die meisten Drucker unterstützen den USB-Anschluss.
8. **D.** Die druckende Anwendung (die Software) ist wahrscheinlich falsch konfiguriert.
9. **A.** Farbsublimationsdrucker verwenden wärmeempfindliche Kunststoffbänder, in die verschiedene Farben eingebettet sind.
10. **C.** Die Druckerwarteschlange hilft Ihnen festzustellen, warum ein Druckauftrag nicht gedruckt wurde.

Computersicherheit 27

Themen in diesem Kapitel:

- Bedrohungen für Ihren Computer und Ihre Daten
- Wichtige Sicherheitskonzepte und -technologien
- Schutz vor Gefahren aus dem Netzwerk

Ihr PC ist in Gefahr. Über Ihren PC können böswillige Personen wertvolle Informationen über Sie und Ihre Gewohnheiten in Erfahrung bringen. Sie können Ihre Dateien stehlen. Sie können Programme ausführen, die Ihre Eingaben aufzeichnen, und damit Benutzernamen und Passwörter, Kreditkartendaten und vieles andere mehr ausspionieren. Sie können Software ausführen, die einen Großteil Ihrer Rechenleistung verbraucht, und Ihren Computer nutzen, um Spam zu versenden oder etwas von anderen zu stehlen. Die Bedrohung ist real und aktuell. Und was noch schlimmer ist: Während ich dies schreibe, werden Ihre Kunden auf dieselbe Weise bedroht. Sie müssen Ihren Computer und Ihre Benutzer vor derartigen Angriffen schützen.

Aber was ist Computersicherheit denn eigentlich? Ein Antivirenprogramm? Lange, komplizierte Kennwörter? Natürlich gehört das auch dazu, aber was ist mit der Tatsache, dass Ihr Laptop ganz einfach gestohlen werden kann? Oder dass ungenügende Belüftung zum Ausfall der Festplatte und anderer Komponenten führen kann?

Um Computer zu schützen, brauchen Sie eine vernünftige Strategie und die richtige Taktik. Aus strategischer Sicht müssen Sie die von unautorisierten Zugriffen auf lokale Rechner ausgehenden Bedrohungen und die mit der Einrichtung eines Netzwerks verbundenen Gefahren verstehen. In diesem Rahmen müssen Sie wissen, wie sich diese Gefahren durch Nutzung von Richtlinien, Programmen und Hardware in Grenzen halten lassen. Aus taktischer Sicht müssen Sie sich mit den Einzelheiten auskennen und die richtigen Werkzeuge implementieren und pflegen können. Sie müssen beispielsweise nicht nur Antivirenprogramme auf den Rechnern der Benutzer installieren, sondern diese Programme auch regelmäßig aktualisieren, um gegen die Flut ständig neuer Schadsoftware gewappnet zu bleiben.

1002

27.1 Bedrohungsanalyse

Ihre Daten und Ihr PC sind auf zweierlei Weise bedroht, nämlich durch Unfälle und durch Aktionen böswilliger Menschen. Es kann alles Mögliche schiefgehen, von einem Benutzer, der Zugriff auf einen Ordner erhält, den er eigentlich nicht sehen sollte, bis hin zu einem Virus, das all Ihre Ordner löscht. Dateien können gelöscht und umbenannt werden oder einfach verloren gehen. Festplattenlaufwerke können ausfallen, und optische Datenträger können zerkratzt und damit unlesbar werden. Unfälle sind einfach unvermeidbar und selbst Menschen, die es nur gut meinen, können Fehler begehen.

Leider gibt es auch viele Leute, die Ihnen absichtlich Böses wollen. Wenn sich Bösartigkeit mit Computerbegabung paart, ist das eine explosive Mischung. Wir werden die folgenden Probleme betrachten:

- Unautorisierter Zugriff
- Social Engineering
- Denial of Service (Dienstblockade)

- Versehentliche oder absichtliche Datenvernichtung
- Administrativer Zugriff
- Katastrophale Hardware-Ausfälle
- Physischer Diebstahl
- Viren und andere Schadsoftware
- Gefährliche Umgebungsbedingungen

27.1.1 Unerlaubter Zugriff

Unautorisierter Zugriff findet statt, wenn ein Benutzer auf unerlaubte Weise auf Ressourcen zugreift. Mit Ressourcen sind in diesem Fall Daten, Programme und Hardware gemeint. Ein Benutzer kann Daten verändern oder löschen, auf sensible Informationen wie etwa Finanzdaten, persönliche Dateien oder E-Mails zugreifen oder einen Computer für Zwecke nutzen, die dessen Eigentümer nicht vorgesehen hat.

Nicht jeder unautorisierte Zugriff geschieht böswillig. Häufig tritt dieses Problem auf, wenn an einem Computer herumexperimentierende Benutzer entdecken, dass sie auf Ressourcen auf eine Art und Weise zugreifen können, die der eigentliche Besitzer nicht vorgesehen hat. Unautorisierter Zugriff wird böswillig, wenn Außenstehende bewusst und absichtlich Schwächen in Ihrem Sicherheitssystem nutzen, um Informationen zu sammeln, Ressourcen zu nutzen oder Daten zu vernichten!

Eine Variante des unautorisierten Zugriffs ist das Eindringen in Computersysteme. Sicherlich können Sie sich vorstellen, wie jemand eine Tür eintritt und sich in einen Computer hackt, viel häufiger handelt es sich aber um jemanden, der zu Hause an seinem Rechner sitzt und die verschiedensten Kennwörter über das Internet ausprobiert. Das ist zwar weniger filmreif, aber ähnlich gefährlich ...

Auch durch das Durchsuchen von Papierkörben und Abfällen (*Dumpster Diving*) können Hacker an Informationen gelangen. Dabei handelt es sich ebenfalls um eine Art Eindringen. Sie würden es nicht glauben, wie viele sensible Daten in die Papierkörbe von Unternehmen wandern! Vor einigen Jahren habe ich mit einem Profi aus dem Bereich der IT-Sicherheit zusammengearbeitet, mit dem ich unsere Büroabfälle untersucht habe. Binnen 20 Minuten hatten wir genügend Informationen gesammelt, um auf das Netzwerk zugreifen und etliche Mitarbeiter ernsthaft unter Druck setzen zu können. Wenn man nach Informationen sucht, wird man im Abfall oft fündig!

Eine andere Vorgehensweise, um unautorisierten Zugriff zu erlangen, ist das schlichte Beobachten des Bildschirms oder der Tastatureingaben. Natürlich muss der Bösewicht Ihnen dabei über die Schulter blicken, aber oft lassen sich Kennwörter bei der Eingabe ganz leicht »mitlesen«.

27.1.2 Social Engineering

Es ist zwar wahrscheinlicher, dass Sie Daten durch Unfälle verlieren, aber die Taten böswilliger Benutzer sorgen für die Mehrzahl der Schlagzeilen. Ein Großteil dieser Angriffe erfolgt unter dem Stichwort *Social Engineering*. Dabei handelt es sich um eine Vorgehensweise, Menschen, die sich legitim innerhalb von Netzwerkumgebungen bewegen dürfen, so zu beeinflussen oder zu manipulieren, dass man von außen Zugriff auf ein Netzwerk erhält. Der Begriff Social Engineering deckt die vielen Methoden ab, mit denen Menschen manipuliert werden können, um unberechtigt an Informationen zu gelangen. Dabei könnte es sich beispielsweise um Anmeldedaten für das Netzwerk, Kreditkartennummern oder Kundendaten handeln – fast alles, was nicht für die Augen unternehmensfremder Personen gedacht ist.

Bei derartigen Manipulationen handelt es sich zumindest im klassischen Sinne nicht um Hacken, auch wenn die Ziele dieselben sind. Nachfolgend sind einige klassische Formen von Social-Engineering-Angriffen beschrieben.

Hinweis

Häufig werden beim Angriff durch Social Engineering verschiedene Methoden kombiniert. Wenn Ihnen also etwas verdächtig erscheint, sollten Sie auf weitere Hinweise achten.

Eindringen

Hacker können in Ihr Gebäude eindringen – und dabei so tun, als hätten sie einen legitimen Grund dafür, wie z.B. als Reinigungspersonal, Handwerker oder Boten getarnt. Sie durchsuchen Schreibtische nach Informationen. Sie könnten auch mit Unternehmensmitarbeitern sprechen, um Namen, Telefonnummern, Abteilungsnamen usw. zu erfahren. Das ist an sich zwar nichts Weltbewegendes, kann aber ein leistungsfähiges Werkzeug sein, wenn diese Informationen später mit anderen Angriffen aus dem Bereich des Social Engineerings kombiniert werden.

Wenn sich böswillige Personen wie legitime Benutzer kleiden und dabei gefälschte Ausweise und andere Hilfsmittel benutzen, können sie sich den unberechtigten Zugang erschleichen und damit potenziell auch an Ihre Daten gelangen. Recht häufig wird versucht, sich unerlaubten Zutritt dadurch zu erschleichen, dass man dicht hinter jemandem hergeht, so tut, als ob man zu ihm gehöre, und mit ihm durch eine Tür oder Schleuse geht. Diese als *Tailgating* bezeichnete Vorgehensweise ist eine gängige Form des Eindringens.

Zum Schutz vor Tailgating gibt es bei vielen Zugängen zu besonders geschützten Bereichen Personenschleusen. Dabei handelt es sich um eine Kabine mit zwei Türen, einer Eingangstür und einer Tür, die zum geschützten Bereich führt. In der Kabine hat nur eine Person Platz, und beim Passieren der Schleuse muss die Eingangstür geschlossen sein, bevor sich die Zugangstür öffnen lässt. Neben der Personenschleuse ist außerdem irgendein Ausweisdokument erforderlich. Um die Sicherheit weiter zu erhöhen, wird die Personenschleuse oft von Wachpersonal kontrolliert, das eine Besucherliste führt, in der alle Personen verzeichnet werden, die das Gebäude betreten oder verlassen.

Die Telefonmasche

Betrügerische Telefonanrufe sind wahrscheinlich die häufigsten Angriffe im Rahmen des Social Engineerings. Dabei ruft der Angreifer irgendjemanden im Unternehmen an, um an Informationen zu gelangen. Der Angreifer versucht, sich als Mitarbeiter des Unternehmens auszugeben, um so die gewünschten Informationen zu erhalten. Am bekanntesten ist die Masche »Ich habe meinen Benutzernamen und mein Passwort vergessen.« Bei dieser Taktik verschafft sich der Angreifer durch Eindringen in das Unternehmen zuerst den Kontennamen eines legitimen Unternehmensmitarbeiters. Anschließend ruft er jemanden im Unternehmen an, häufig einen Supportmitarbeiter, um weitere Informationen zu erhalten, in diesem Fall ein Passwort.

Hacker: »Hi, hier ist Hans-Hermann Dampf aus der Buchhaltung. Ich habe mein Kennwort vergessen. Könnten Sie es bitte zurücksetzen?«

Support: »Natürlich. Wie lautet Ihr Benutzername?«

Hacker: »h_h_dampf.«

Support: »OK, ich setze es auf e34rd3.«

Natürlich sind solche telefonischen Betrügereien nicht auf den Zugang zum Netzwerk beschränkt. Oft geht es auch um Bargeld, Material für Erpressungen und andere wertvolle Dinge.

Phishing

Beim *Phishing* handelt es sich um den Versuch, Benutzer auf elektronischem Wege zur Preisgabe ihrer Benutzernamen, Kennwörter und anderer Sicherheitsinformationen zu verleiten. Ein klassisches Beispiel stellen E-Mails dar, die angeblich von Ihrer Bank stammen und in denen Sie zum Aufsuchen einer fingierten Webseite und zur Angabe Ihres Benutzernamens und Kennworts aufgefordert werden. Beim Phishing handelt es sich heute um die weitaus häufigste Form des Social Engineerings.

Phishing ist eine Betrugsform, die eher durch Zufall funktioniert, denn der Betrüger hat es auf beliebige Personen abgesehen, die dumm genug sind, den Köder zu schlucken. Der Begriff *Spear Phishing* beschreibt hingegen eine ganz gezielte Angriffsform, beispielsweise wenn ein Bösewicht es auf einen ganz bestimmten Prominenten abgesehen hat. Das Gefährliche beim Spear Phishing ist, dass der Köder anhand bekannter Details aus dem Leben des Angriffsziels äußerst sorgfältig maßgeschneidert werden kann.

27.1.3 Denial of Service

Bei einem *Denial-of-Service*-Angriff werden verschiedene Methoden eingesetzt, um ein System in die Knie zu zwingen, sodass es praktisch nicht mehr funktioniert, etwa einen Webserver. DoS-Angriffe waren in der Frühzeit des Webs relativ häufig. Heutzutage gibt es *Distributed-Denial-of-Service*-Angriffe (DDoS-Angriffe), bei denen sehr viele Computer gleichzeitig eingesetzt werden, um ein System lahmzulegen.

27.1.4 Datenvernichtung

Häufig sorgen erweiterte unautorisierte Zugriffe, bei denen Daten zerstört werden, für sehr viel mehr als nur absichtlich oder versehentlich gelöschte oder beschädigte Daten. Man kann sich leicht vorstellen, dass sich ein böswilliger Hacker Zugriff auf Ihr Netzwerk verschafft und alle Ihre wichtigen Dateien löscht, aber denken Sie an den Fall, wo berechtigte Benutzer auf bestimmte Daten zugreifen, aber mit diesen Daten mehr tun, als sie eigentlich dürften. Ein gutes Beispiel dafür ist jemand, der berechtigt auf eine Produktdatenbank zugreift, um Produktbeschreibungen zu ändern, und dann feststellt, dass er auch die Produktpreise ändern kann.

Diese Art Bedrohung ist vor allem dann gefährlich, wenn Benutzer nicht klar darüber informiert wurden, in welchem Umfang sie Änderungen vornehmen dürfen. Ein befreundeter Techniker erzählte mir einmal von einem Benutzer, der in eine wichtige Datenbank gelangen konnte, weil ihm jemand falsche Zugriffsrechte erteilt hatte. Als er darauf angesprochen wurde, sagte der Benutzer: »Wenn ich die Änderung nicht hätte durchführen dürfen, hätte es mir das System nicht erlaubt!« Viele Benutzer glauben, dass Systeme so restriktiv eingerichtet werden, dass sie einfach unerlaubte Aktionen nicht zulassen. Deshalb gehen Benutzer häufig davon aus, dass sie zu Änderungen berechtigt sind, die sie für notwendig halten, sofern ihnen nur der Zugriff auf die Daten erlaubt ist.

27.1.5 Administrativer Zugriff

Unter allen modernen Betriebssystemen können Sie Benutzerkonten anlegen und Dateien und Ordnern auf dem Rechner bestimmte Zugriffsrechte zuweisen. Als Administrator oder Root-Benutzer haben Sie volle Kontrolle über praktisch alle Aspekte des Computers. Diese erhöhten Berechtigungen bedeuten, dass erhebliche größere Schäden angerichtet werden können, falls solch ein Benutzerkonto kompromittiert wird. Daher sollte es das Ziel sein, sowohl die Anzahl als auch die Nutzungsdauer solcher Benutzerkonten zu minimieren.

Selbst wenn ein Benutzer diese erweiterten Rechte unbedingt benötigt, vernünftige Kennwörter benutzt und für physische Sicherheit sorgt, ist es dennoch möglich, dass ein überzeugender Spear-Phishing-Angriff erfolgreich ist. Die auf diese Weise installierte Schadsoftware könnte dann auf Dateien zugreifen, Software installieren und Einstellungen ändern, also Dinge tun, die einem einfachen Benutzerkonto nicht gestattet wären.

27.1.6 Systemabstürze/Hardware-Ausfälle

Wie jede Technologie können und werden Computer ausfallen – normalerweise dann, wenn es am wenigsten passt. Festplatten geben ihren Geist auf, der Strom fällt aus – das gehört im Computerbereich zum Alltag. In anfälligen Bereichen müssen Sie für Redundanzen (z.B. eine USV für den Fall des

Stromausfalls) und vor allem für die Durchführung der überaus wichtigen Datensicherungen sorgen. In Kapitel 14 erfahren Sie mehr über Datensicherung und andere bedeutsame Aspekte, die für stabil und zuverlässig arbeitende Systeme erforderlich sind.

27.1.7 Physischer Diebstahl

Ein im Netzwerkbereich tätiger Freund forderte mich einmal auf, zu versuchen, sein neu installiertes Netzwerk zum Absturz zu bringen. Er hatte gerade einen leistungsfähigen und teuren Firewall-Router installiert und war davon überzeugt, dass ich nicht auf einen Test-Server gelangen könnte, den er seinem Netzwerk extra für mich hinzugefügt hatte. Nach ein paar Versuchen, über das Internet einzudringen, erkannte ich, dass ich auf diese Weise nicht weit kommen würde.

Ich stieg also in mein Auto und fuhr zu seinem Büro. Dabei trug ich meinen sehr nach Techniker aussehenden Overall und eine alte Ausweiskarte, die ich in einer Schublade herumliegen hatte. Ich lächelte die Dame am Empfang freundlich an und ging direkt am Büro meines Freundes vorbei (mir fiel auf, dass er selbstgefällig allen eingehenden IP-Verkehr über ein Paket-Sniffing-Programm überwachte) zu seinem neuen Server.

Ich zog schnell die Leitungen von seinem kostbaren neuen Gerät ab, schnappte es mir und ging wieder hinaus. Die Dame am Empfang war viel zu sehr damit beschäftigt herauszufinden, warum ihr E-Mail-Programm nicht mehr funktionierte, als dass sie gesehen hätte, wie ich den 30 Kilo schweren Server hinaustrug. Ich stellte ihn im Vorzimmer ab und rief meinen Freund von meinem Handy aus an:

Ich (fröhlich): »Geschafft, ich habe alle deine Daten!«

Er (weniger fröhlich): »Du hast meinen Server neu gebootet! Wie hast du das gemacht?«

Ich (grinsend): »Ich habe ihn nicht gebootet – sieh nach!«

Er (jetzt richtig wütend): »DU <KRAFTAUSDRUCK> DIEB! DU HAST MEINEN SERVER GESTOHLEN!«

Ich (herzlich): »Ja, genau. Gib mir zwei Tage, bis ich zu Hause in aller Ruhe dein Passwort herausgefunden habe, dann werde ich alles sehen. Bis dann!«

Ich ging sofort wieder zurück und übergab ihm den Server. War alles ja nur ein Spaß. Aber man kann daraus lernen: Vergessen Sie nie, dass die beste Sicherheitssoftware für das Netzwerk sinnlos sein kann, wenn Ihre Systeme physisch ungeschützt bleiben!

Hinweis

Die physische Sicherheit Ihrer Systeme betrifft mitnichten nur die Geräte im Büro. Die Tatsache, dass Laptops tragbar sind, ist auch dafür verantwortlich, dass sie für Diebe so interessant sind. Eine einfache Maßnahme zum Schutz Ihres Laptops ist der Einsatz eines Sicherungskabels, das um unbewegliche Gegenstände geschlungen wird und am Laptop angeschlossen wird.

27.1.8 Viren und andere Schadsoftware

Netzwerke sind zweifellos die schnellsten und effizientesten Transportmittel für die Übertragung von Computerviren zwischen Systemen. In den Nachrichten geht es hauptsächlich um die vielen Angriffe durch Schadsoftware aus dem Internet, aber viel Schadsoftware stammt immer noch von Benutzern, die Programme auf optischen Datenträgern und USB-Speicherticks einschleppen. Dieses Kapitel beschreibt die verschiedenen Infektionsmethoden mit Viren und Schadsoftware, und im Abschnitt 27.3, *Netzwerksicherheit*, darüber hinaus, was Sie tun müssen, um sich vor einer Infektion Ihrer vernetzten Systeme zu schützen.

27.1.9 Gefährliche Umgebungsbedingungen

Ihr Computer ist von allen möglichen gefährlichen Dingen umgeben, die nur darauf warten, ihm zu schaden: schwankende Stromversorgung durch die Elektrizitätswerke, jede Menge Chemikalien, die Sie möglicherweise aus betrieblichen Gründen in der Nähe des Computers lagern müssen, Staub, Hitze, Kälte, Nässe ... es ist die Hölle!

Wichtig

Rechnen Sie in den CompTIA A+-Prüfungen mit Fragen zum Thema Umgebungsbedingungen.

Stromversorgung

Die Stromversorgung wurde in Kapitel 7 bereits ausführlich erläutert. Vergessen Sie jedoch nie, wie wichtig Überspannungsschutz und USV (Unterbrechungsfreie Stromversorgung) sind, um Ihre Geräte vor Spannungsschwankungen und Stromausfällen zu schützen. Beachten Sie ebenfalls, dass auch Netzwerkkomponenten einen solchen Schutz benötigen. Abbildung 27.1 zeigt eine USV im Rack.



Abb. 27.1: Unterbrechungsfreie Stromversorgung

Klimatisierung

Eine angemessene Klimatisierung schützt Server und Arbeitsplatzrechner vor Umwelteinflüssen wie Hitze, Staub und Feuchtigkeit. Zur Kontrolle der Umgebungsbedingungen gehören neben einer Klimaanlage auch Belüftung, Luftfilterung und die Überwachung von Temperatur und Luftfeuchtigkeit. Als Techniker sollten Sie ein gewisses Gespür dafür besitzen, wenn hier bestimmte Grenzwerte überschritten werden.

Zimmertemperatur und saubere, trockene Luft sind die geeigneten Umgebungsbedingungen für einen PC. Die CompTIA erwartet von Ihnen nicht die Kenntnisse eines Umwelttechnikers, aber dass verunreinigte, feuchte oder zu heiße Luft negative Auswirkungen auf den Betrieb eines Computers haben, sollten Sie schon wissen. Da diese Aspekte in verschiedenen Teilen des Buches bereits Erwähnung finden, folgt hier eine kurze Zusammenfassung vor dem Hintergrund der Sicherheit.

Verunreinigte Luft Staub und Ablagerungen tun keinem elektronischen Bauteil gut. Eine typische Büroklimatisierung ist in den meisten Fällen ausreichend, aber nicht alle Computer befinden sich in solchen Räumen. Es spielt keine Rolle, wo sich der Computer befindet, er darf nicht verunreinigt werden. Am besten führen Sie regelmäßige Kontrollen durch. Staub und Ablagerungen finden sich überall, jedoch sind Lüfter besonders betroffen, da sich Staub und Verschmutzungen hier regelrecht ansammeln (Abbildung 27.2).

Eine Verunreinigung der elektronischen Komponenten im Laufe der Zeit ist nahezu unvermeidbar. Zur Reinigung können Sie entweder Druckluftspray oder einen Staubsauger verwenden. Welche Methode ist besser? Es gibt eine einfache Regel: Wenn es nicht stört (wie etwa vor der Haustür), dass der aufgewirbelte Staub umherfliegt, sollten Sie Druckluft verwenden, anderenfalls einen Staubsauger.

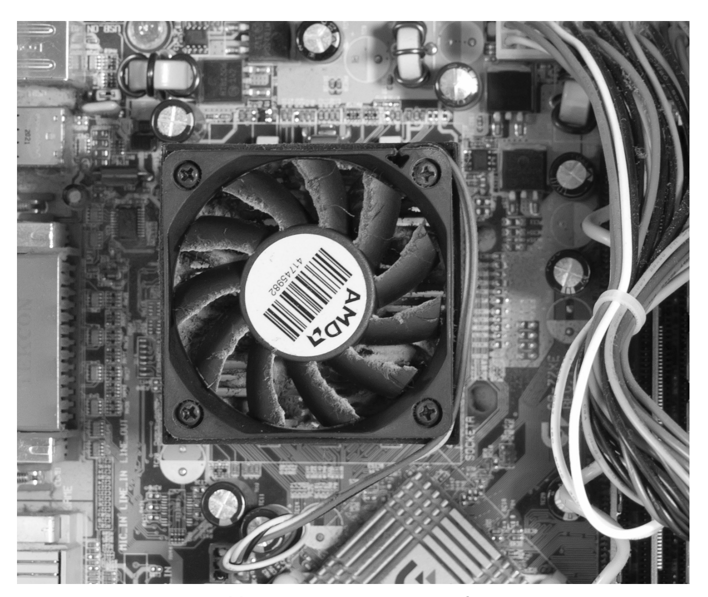


Abb. 27.2: Verunreinigter Lüfter

Räume mit Geräte-Racks müssen ausreichend belüftet und klimatisiert sein (Abbildung 27.3). Stellen Sie außerdem sicher, dass die Luftfilter der Klimaanlage regelmäßig erneuert werden.



Abb. 27.3: Lüfterabdeckung der Klimaanlage in einem Serverschrank

Bei wirklich widrigen Umgebungsbedingungen gibt es die Möglichkeit, einen Staubschutzschrank zu verwenden. Ein solcher Schrank besitzt einen eigenen Luftfilter und erlaubt es, einen Computer auch unter den lausigsten Umgebungsbedingungen zu betreiben.

Wichtig

Sorgen Sie immer für ausreichende Belüftung, funktionsfähige Luftfilter und halten Sie die Serverschränke geschlossen. Tragen Sie gegebenenfalls eine Atemschutzmaske, um sich vor Staubpartikeln in der Luft zu schützen.

Temperatur und Luftfeuchtigkeit Die meisten Computer sind für den Betrieb bei Zimmertemperatur (ca. 22° Celsius) und einer relativen Luftfeuchtigkeit von etwa 30 bis 40% ausgelegt. Zwar haben es Computer gerne kühler und trockener, die Menschen, die daran arbeiten, allerdings nicht. Probleme gibt es also nur, wenn es wärmer und feuchter wird.

Moderne Büroumgebungen sind im Allgemeinen gut klimatisiert (oder beheizt), weshalb es Ihre Aufgabe als Techniker ist, dafür zu sorgen, dass die Klimatisierung ordnungsgemäß arbeitet. Sie sind sozusagen ständig auf Streife, um die Belüftung zu überwachen. Beachten Sie Folgendes:

- Stellen Sie sicher, dass die Schächte der Klimaanlage nicht versperrt oder zugestellt sind.
- Prüfen Sie gelegentlich die Temperatur der Rohrleitungen (diese dürfen nicht zu warm oder zu kalt sein).
- Achten Sie darauf, dass einzelne Geräte nicht zu weit von der Klimatisierung entfernt sind.

Giftige Substanzen

In jedem Büro gibt es die unterschiedlichsten chemischen Substanzen, die gesundheitsgefährdend sind. Manche davon stellen eine unmittelbare Bedrohung dar – sie können in Flammen aufgehen oder Haut, Lunge und Augen verätzen. Andere sind krebserregend oder gefährden die Gesundheit auf andere Weise, wenn man ihnen jahrelang ausgesetzt ist. Den Lernzielen der CompTIA A+-Prüfung 1002 zufolge sollten Sie die gesetzlichen Umweltschutzbestimmungen für den Umgang mit solchen Substanzen kennen.

Umweltschutzbestimmungen klingen zunächst einmal einschüchternd, haben aber ein einfaches Ziel: Die Menschen, die mit oder in der Nähe solcher Substanzen arbeiten, müssen die Risiken kennen, wissen, welche Vorsichtsmaßnahmen sie treffen sollten und was bei einem Unfall zu tun ist. Sie sollten sich über die Bestimmungen informieren und sich daran halten. Zumindest jedoch sollten Sie das Sicherheitsdatenblatt (MSDS, Material Safety Data Sheet) für Substanzen, mit denen Sie regelmäßig arbeiten, gelesen haben, ein Dokument, das die Risiken, Vorsichtsmaßnahmen und die Reinigungs- bzw. Entsorgungsverfahren ausführlich beschreibt. Sie sollten auch wissen, wo das Sicherheitsdatenblatt zu finden ist, wenn Sie etwas verschüttet haben und Sie sich nicht darüber im Klaren sind, wie damit umzugehen ist.

Wichtig

In allen größeren Städten gibt es Annahmestellen für derartige Substanzen, die auch elektronische Bauteile fachgerecht entsorgen oder recyceln. Suchen Sie im Internet nach dem Stichwort »Annahmestelle« und dem Namen Ihres Wohnorts, um diese ausfindig zu machen.

27.2 Sicherheitskonzepte und -technologien

Sobald Sie die Bedrohung für Ihre Computer und Ihr Netzwerk einschätzen können, müssen Sie Maßnahmen zum Schutz dieser wertvollen Ressourcen ergreifen. Je nach Größe Ihres Unternehmens kann das eine einfache Aufgabe sein, die nur einige grundlegende Sicherheitskonzepte und Vorgehensweisen umfasst, es kann sich aber auch um eine außerordentlich komplizierte Angelegenheit handeln. Die Sicherheitsbedürfnisse für ein aus drei Personen bestehendes Desktop-Publishing-Unternehmen würden sich beispielsweise sehr von denen eines Unternehmens unterscheiden, das den Bundesnachrichtendienst mit streng geheimen Spielzeugen beliefert.

Aus der Sicht eines CompTIA A+-zertifizierten Technikers müssen Sie das Gesamtkonzept und dessen strategische Seite verstehen und die Einzelkonzepte und verfügbaren Sicherheitstechnologien kennen. Auf der Implementierungsebene (der taktischen Seite) müssen Sie wissen, wo die Sicherheitsrichtlinien unter Windows zu finden sind. Ein Techniker mit CompTIA Network+- oder CompTIA Security+-Zertifikat wird Ihnen sagen, welche speziellen Optionen Sie implementieren müssen. (Die Ausnahme stellt hier der Umgang mit bösartiger Software wie Viren dar, dem wir uns aber in der zweiten Hälfte dieses Kapitels zuwenden werden.) Sehen wir uns also die vier konzeptionellen und technologischen Bereiche an: Zugriffskontrolle, Datenklassifizierung und Konformität, Lizenzierung sowie Berichte.

27.2.1 Zugriffskontrolle

Zugriff ist alles. Wenn Sie den Zugriff auf Daten, Programme und andere Rechnerressourcen kontrollieren können, haben Sie ein sicheres System. Die *Zugriffskontrolle* besteht aus miteinander verknüpften Bereichen, über die sich ein guter, sicherheitsbewusster Techniker Gedanken machen sollte: physische Sicherheit, Authentifizierung, Benutzer und Gruppen sowie Sicherheitsrichtlinien. Einen Großteil davon kennen Sie bereits aus früheren Kapiteln, aber dieser Abschnitt hilft Ihnen, alles im Hinblick auf die Sicherheit zu kombinieren.

Physische Sicherheitsbereiche

Die erste Sicherheitsregel besteht darin, den Zugang zur physischen Hardware zu beschränken. Der Markt für Sicherheitstechnik ist riesig, aber im Wesentlichen kommt es auf Folgendes an: Türen, Schlösser, Alarmsysteme und ein wachsames Auge. Zunächst einmal muss man sich darüber im Klaren sein, dass sich alle Sicherheitssysteme irgendwie überwinden lassen. Vernünftige Sicherheit ist äußerst vielschichtig, und die einzelnen Teile können so eingesetzt werden, dass die Stärken betont und die Schwachstellen kompensiert werden.

Denken Sie an die vorhin erwähnten Personenschleusen. Eine einfache Lösung, wie ein klassisches Türschloss, stellt für einen Profi mit dem richtigen Werkzeug, der einen Moment unbeobachtet ist, kaum ein Hindernis dar. Bei einer Personenschleuse werden einfache Sicherheitsmaßnahmen, wie Türen, Türschlösser, Sicherheitspersonal und eine Besucherliste, auf eine Art und Weise miteinander kombiniert, die viel schwieriger zu überwinden ist als abgeschlossene Türen.

Klassische Türschlösser sind besser als nichts, aber Schlüssel können leicht nachgemacht werden, und die Kosten für den Austausch von Schlössern summieren sich schnell. In größeren Unternehmen finden zunehmend Ausweiskarten Verbreitung, die oft der Eingangskontrolle dienen, aber insbesondere auch mit RFID-Chips (*Radio Frequency Identification*) zur persönlichen Identifizierung ausgerüstet sind (siehe nachfolgenden Abschnitt *Authentifizierung*). Abbildung 27.4 zeigt eine solche Ausweiskarte.



Abb. 27.4: Ausweiskarte für Mitarbeiter

Sperrsysteme

Wenn ein Angreifer erst einmal Zugang zu einem Gebäude erlangt hat, ist es sehr viel schwieriger, die Hardware zu schützen. Hier gibt es verschiedene Optionen, aber glauben Sie nicht, dass sie einen versierten Angreifer länger als ein paar Minuten aufhalten. Immerhin machen sie es offensichtlich, dass Böses vor sich geht, wenn beobachtet wird, wie jemand versucht, solche Sicherheitsmaßnahmen zu überwinden.

- Verriegeln Sie die Tür Ihres Arbeitsplatzes. Mit einem verlässlichen System ohne Schlüssel ist das mühelos möglich, selbst wenn man das Büro nur für einen Augenblick verlässt.
- Abschließbare Sicherungskabel verhindern, dass jemand auf die Schnelle Hardware einfach mitnimmt.
- USB-Anschlusssicherungen erschweren es, ein USB-Laufwerk oder einen Speicherstick anzuschließen, um Schadsoftware zu installieren.
- RJ-45-Anschlusssicherungen verhindern, dass ein Angreifer problemlos Zugang zum Netzwerk erhält.
- Server-Sicherungen beschränken den Zugang zu den Anschlüssen und Laufwerken eines Servers. Es gibt auch Server-Racks mit abschließbaren Türen, die den Zugang zur Vorder- oder Rückseite des gesamten Racks verhindern.

Solche Sicherungen sind nutzlos, wenn jemand einfach so hereinspazieren und sich an einen Computer setzen kann, an dem noch ein Benutzer angemeldet ist. Lassen Sie ein angemeldetes System nicht unbeaufsichtigt, auch wenn nur ein Standardbenutzer oder ein Gast angemeldet ist. Und wenn Sie einen Server verlassen, an dem Sie noch als Administrator angemeldet sind, hilft nur noch beten. Sie fordern das Schicksal heraus.

Wenn Sie Ihren Arbeitsplatz für einen Moment verlassen müssen, sollten Sie den Bildschirm sperren, entweder durch ein Tastenkürzel oder durch den entsprechenden Menüpunkt des Betriebssystems. Drücken Sie `Strg` + `L` auf der Tastatur, um das System zu sperren. Das funktioniert unter allen Windows-Versionen. Es ist auch keine schlechte Idee, den Kennwortschutz des Bildschirmschoners mit einer kurzen Wartezeit einzurichten. Ist dieser aktiv, kann der Benutzer erst nach Eingabe eines Kennworts zum Desktop zurückkehren.

Wichtig

Wenn Sie für die Sicherheit mehrerer Benutzer zuständig sind, sollte es eine Richtlinie geben, dass auf jedem Arbeitsplatzrechner der Kennwortschutz des Bildschirmschoners eingerichtet sein muss und so konfiguriert ist, dass der Anmeldebildschirm angezeigt wird, wenn man die Arbeit fortsetzen möchte. Das ist äußerst hilfreich, wenn die Benutzer vergessen, ihren Computer zu sperren, wenn sie eine Pause machen oder zum Mittagessen gehen. Windows und macOS gehen noch einen Schritt weiter und ermöglichen es, eine Zeitspanne anzugeben, nach der bei Untätigkeit automatisch der Bildschirmschoner aktiviert wird.

Schutz sensibler Informationen

Unbeaufsichtigte Systeme durch eine automatische Sperre zu schützen, ist nur vernünftig, bringt aber wenig, wenn es dem Eindringling gelingt, dem Benutzer bei der Eingabe des Kennworts über die Schulter oder auf die Finger zu sehen oder es von einer am Bildschirm angebrachten Haftnotiz abzulesen. Schreiben Sie Kennwörter nicht auf und lassen Sie sie nicht gut sichtbar herumliegen. Erklären Sie den Benutzern, wie man sich leicht zu merkende Kennwörter ausdenken kann (wie in Kapitel 14 beschrieben). Und seien Sie sich des Risikos durch das Mitlesen von Kennwörtern bei der Eingabe bewusst. Idealerweise sind die Büroräume so eingerichtet, dass ein unbemerktes Mitlesen bei Eingabe gar nicht möglich ist.

Für den Fall, dass Benutzer in leicht einsehbaren Bereichen mit sensiblen Daten arbeiten müssen, gibt es spezielle Filter, die vor dem Bildschirm angebracht werden, die den Sichtwinkel einschränken und

es somit verhindern, den Bildschirminhalt zu erkennen, solange man nicht direkt davor sitzt (Abbildung 27.5). Ausgedruckte Dokumente mit persönlichen oder vertraulichen Inhalten sollten nicht offen herumliegen, sondern stattdessen sicher verschlossen verwahrt werden. Und nicht mehr benötigte Dokumente gehören in den Reißwolf.



Abb. 27.5: Der Filter verhindert es, den Bildschirminhalt von der Seite aus zu erkennen.

MAC-Adressen filtern

Es ist zwar bei Weitem nicht wasserdicht, aber wenn ein Angreifer physischen Zugang zu Ihren Räumlichkeiten erlangt, können Sie ihm einen weiteren Stein in den Weg legen, wenn er mit seinen eigenen Geräten auf Ihr Netzwerk zugreifen will. Sowohl kabelgebundene als auch drahtlose Netzwerke unterstützen das Filtern nach MAC-Adressen. Sie können anhand der MAC-Adresse eines Geräts den Zugang zum Netzwerk entweder verweigern oder aber gewähren.

Das Verfahren ist aber nicht wasserdicht, weil ein versierter Angreifer die MAC-Adresse eines Geräts fälschen kann. Dabei ist es sehr viel einfacher, eine gültige WLAN-MAC-Adresse abzuhören als eine kabelgebundene.

Jedenfalls ist es von großem Vorteil, Geräte aus dem Netzwerk fernzuhalten, die nicht unter der eigenen Kontrolle stehen. Wenn es dem Angreifer nicht gelingt, mit einem seiner eigenen Geräte (die vermutlich mit weiteren Angriffswerkzeugen ausgestattet sind) auf das Netzwerk zuzugreifen, ist er gezwungen, in eines Ihrer Geräte einzudringen, um seine Untaten zu verüben.

Authentifizierung

Sicherheit beginnt mit einer korrekt implementierten Authentifizierung, d.h. im Wesentlichen, wie der Computer feststellen kann, wer auf was wie zugreifen darf. Die *Authentifizierung* kann über Hardware und/oder Software erfolgen.

Die Authentifizierung lässt sich grob in drei verschiedene Kategorien unterteilen: Wissen, Besitz und Biometrie. In Kapitel 25 haben Sie im Rahmen der Sicherheit von mobilen Geräten die Mehrfaktor-Authentifizierung bereits kennengelernt, daher muss sie an dieser Stelle nicht näher erläutert werden. Jedenfalls wird sie auch zum Schutz von Desktop-PCs, Laptops, Servern oder Gebäuden eingesetzt. Erwähnenswert ist jedoch, dass viele Unternehmen und Organisationen eine *Zwei-Faktor-Authentifizierung* verwenden. Ein Beispiel hierfür ist ein kleines Gerät in Form eines Schlüsselanhängers, das numerische Codes erzeugt. Der Benutzer authentifiziert sich durch Eingabe von Benutzername und Kennwort (Faktor Wissen) sowie der auf dem Schlüsselanhänger angezeigten Nummer (Faktor Besitz), wenn er dazu aufgefordert wird.

Wichtig

In der Zertifizierungsprüfung 1002 können Fragen zur Zwei-Faktor- und Mehrfaktor-Authentifizierung vorkommen. Sie betrifft alle computerähnlichen Geräte.

Software-Authentifizierung: Die richtige Kennwortwahl Ich bin immer wieder fassungslos, wenn ich den Computer eines Freundes einschalte und dann direkt auf seinen Desktop gelange oder wenn ich bei verheirateten Freunden mit Kindern auf eines der Benutzerkontensymbole klicke und nicht nach einem Kennwort gefragt werde. Das ist einfach nicht in Ordnung! Ich bin immer versucht, sofort Kennwörter einzurichten, ohne sie ihnen zu verraten, damit sie ihren Fehler einsehen, wenn sie sich wieder anmelden wollen. Ich mache das natürlich nicht, aber ich versuche zumindest immer, die Bedeutung von guten Kennwörtern zu erklären.

Wichtig

Merkwürdigerweise ist in den Lernzielen der CompTIA A+-Prüfung 1002 die *Wiederherstellungskonsole* als brauchbares Sicherheitswerkzeug aufgeführt, aber das galt nur für Windows XP, nicht für die Betriebssysteme der aktuellen Prüfungen. Die Wiederherstellungskonsole könnte also als falsche Antwort vorkommen.

Aus Kapitel 13 wissen Sie bereits alles Wichtige über Kennwörter, daher soll es an dieser Stelle genügen, darauf hinzuweisen, dass Ihre Benutzer vernünftige Kennwörter benutzen müssen. Stellen Sie außerdem sicher, dass die Kennwörter regelmäßig erneuert werden. Und achten Sie darauf, dass die Benutzer sich die Kennwörter nicht aufschreiben und sie auch nicht unter ihre Mauspads kleben!

Sie müssen übrigens nicht nur an den Zugriff auf Windows denken. Wenn Computer öffentlich zugänglich aufgestellt werden, dann gibt es immer Leute, die in das System einzudringen versuchen, Unfug damit anstellen und z.B. die CMOS-Einstellungen ändern, das Gehäuse öffnen oder sogar Festplatten stehlen. Der Rechner lässt sich dann erst wieder normal benutzen, wenn ein Techniker den Schaden behoben hat. Alle modernen CMOS-Setup-Programme enthalten eine Reihe von Vorkehrungen zum Schutz des Rechners, wie z.B. Laufwerkverriegelung, Einbruchserkennung beim Gehäuse und natürlich BIOS/UEFI-Kennwörter (Abbildung 27.6). Wenn Sie noch einmal nachlesen wollen, was Sie auf der BIOS-Ebene zum Schutz Ihres Rechners unternehmen können, dann lesen Sie noch einmal in Kapitel 5, *BIOS und CMOS*, nach.

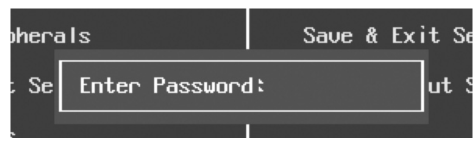


Abb. 27.6: BIOS/UEFI-Kennwortabfrage

Hardware-Authentifizierung Tore, Türen und Computer können Kartenleser und biometrische Geräte verwenden, um Benutzer zuverlässiger zu authentifizieren als nur durch reine Kennwörter. Smartcards sind kreditkartengroße Karten mit einem Chip, der den Karteninhaber identifiziert. Smartcards sind zwar allgemein relativ verbreitet und dienen z.B. der Authentifizierung von Benutzern bei Eingangskontrollsystemen, werden im Computerbereich aber eher selten genutzt. Abbildung 27.7 zeigt eine Tastatur mit Smartcard-Lesegerät.

Bei einem *Sicherheits-Token* handelt es sich um ein kleines Gerät in der Größe und Form eines Schlüsselanhängers, das der Benutzer bei sich trägt. Auf ihm sind Informationen wie digitale Zertifikate, Kennwörter, biometrische Daten oder RSA-Token gespeichert. *RSA-Token* erzeugen zufällige Zahlenkombinationen, die gemeinsam mit Benutzername und Kennwort zur Erhöhung der Sicherheit eingesetzt werden (Abbildung 27.8).



Abb. 27.7: Smartcard und Tastatur mit Lesegerät (Foto mit freundlicher Genehmigung von Cherry)



Abb. 27.8: RSA-Token (Foto mit freundlicher Genehmigung von EMC)

Viele Sicherheits-Token werden auch als Software bereitgestellt. Wenn Sie *World of Warcraft* spielen, wissen Sie auch, dass es die sogenannten *Gold Farmer* gibt, die sich in die Benutzerkonten einhacken und die Spieler um die wohlverdiente Beute bringen, die sie beim Spielen gesammelt haben. Es ist ein furchtbares Gefühl, sich dort anzumelden, nur um festzustellen, dass man ausgeplündert wurde (Abbildung 27.9).



Abb. 27.9: Überfall! Waffen weg, Taschen leer, Konto geplündert!

Um diesen Problemen etwas entgegenzusetzen, stellte Blizzard Entertainment, der Hersteller des Spiels, kostenlose Sicherheits-Tokens bereit. Die meisten Leute denken beim Begriff *Sicherheits-Token* an Hardware in Form eines Schlüsselanhängers, aber ein Sicherheits-Token kann man auch in Form von Software herunterladen. Blizzard bietet hierfür eine Smartphone-App an (Abbildung 27.10).

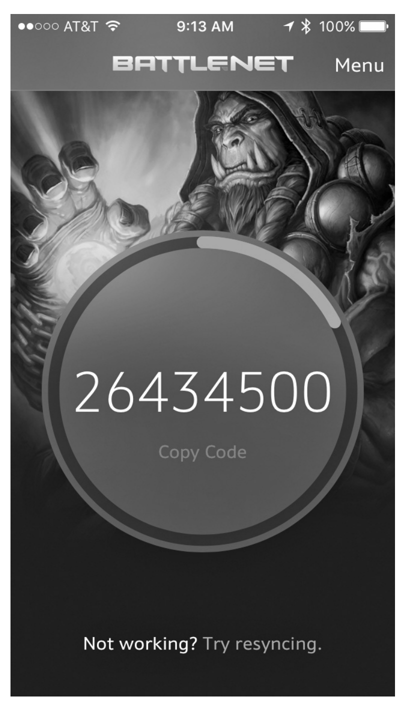


Abb. 27.10: Das Sicherheits-Token von Blizzard Entertainment für das iPhone

Man kann zwar Kennwörter erraten oder herausfinden, aber es ist schon sehr viel schwerer, Fingerabdrücke zu fälschen. Die Tastatur in Abbildung 27.11 authentifiziert Benutzer eines Rechners über deren Fingerabdrücke.



Abb. 27.11: Microsoft-Tastatur mit Fingerabdruckscanner

Andere Geräte, die eine vergleichbare Sicherheit bieten, sind RFID-Schlüsselanhänger oder Netzhautscanner. Geräte, bei denen die Authentifizierung durch irgendwelche körperlichen Merkmale erfolgt, werden *biometrische Geräte* genannt.

Hinweis

Und wie wäre es jetzt mit einer Enthüllung? Microsoft behauptet nicht, dass die Tastatur in Abbildung 27.11 überhaupt für Sicherheit sorgt. Die Dokumentation besagt ausdrücklich, dass es sich beim Fingerabdruckscanner um ein Zugriffswerkzeug und keine Sicherheitsvorkehrung handelt. Weil er einer Person aber die Anmeldung bei einem Rechner ermöglicht, gehört er meiner Ansicht nach sehr wohl in die Kategorie der Authentifizierungsgeräte.

Geschäftstüchtige Hersteller haben Schlüsselanhänger und Smartcards entwickelt, die mit *Funkfrequenzkennungen* (RFID – Radio Frequency Identification) arbeiten, um Authentifizierungsdaten zu übertragen, damit Benutzer nichts mehr in den Computer oder in den Kartenleser einstecken müssen. Der *Privaris plusID* beispielsweise kombiniert einen biometrischen Fingerabdruck-Schlüsselanhänger mit einem RFID-Sender, mit dem sich beispielsweise ein Garagentor ferngesteuert öffnen lässt.

In den Medien ist immer wieder von *Netzhautscannern* die Rede, wenn es um biometrische Geräte zur Erhöhung der Sicherheit geht. Nun gibt es Netzhautscanner durchaus, allerdings ist mir in fast 30 Berufsjahren als Techniker und in Hunderten von hochgradig gesicherten Anlagen nur ein einziges Mal ein solches Gerät begegnet. Daher wird Abbildung 27.12 vermutlich die einzige eines Netzhautscanners in Aktion sein, die Ihnen jemals unterkommen wird.



Abb. 27.12: Netzhautscanner in Half-Life 2

Aktuelle Smartphones und Tablets verwenden eine Gesichtserkennung zur Identifizierung und Authentifizierung, allerdings kann auch eine PIN verwendet werden, wenn die Erkennung fehlschlägt. Abbildung 27.13 zeigt einen Benutzer, der sich durch Gesichtserkennung an einem iPhone

anmeldet. (Beachten Sie das geöffnete Schloss. Der Vorgang lässt sich nur schwer abbilden, weil er so schnell vor sich geht.)



Abb. 27.13: Entsperren eines iPhones durch Gesichtserkennung

Benutzer und Gruppen

Windows verwendet *Benutzerkonten* und *Benutzergruppen* als Grundlage der Zugriffskontrolle. Ein Benutzerkonto wird einer Gruppe (z.B. Benutzer, Hauptbenutzer oder Administratoren) zugeordnet und erhält dadurch bestimmte Berechtigungen auf dem Computer. Der Einsatz von NTFS bietet die bestmögliche Kontrolle der Datenressourcen.

Die Zuordnung von Benutzern zu Gruppen ist ein wichtiger erster Schritt zur Kontrolle eines lokalen Rechners, aber diese Funktion kann erst dann wirklich glänzen, wenn sie in einer vernetzten Umgebung eingesetzt wird. Das wollen wir uns jetzt einmal genauer ansehen.

Hinweis

Wenn es um die Sicherheit geht, dann spielt das Dateisystem der Festplatten eine wichtige Rolle. Die Dateisysteme des Startlaufwerks aller aktuellen Betriebssysteme unterstützen *Zugriffssteuerungslisten*, eine erweiterte Form von Zugriffsrechten für Benutzer und Gruppen. Die dadurch gewährleistete Sicherheit gilt jedoch nur für Laufwerke, die mit einem der modernen Dateisysteme wie NTFS, HFS+ oder ext3/4 formatiert sind. Wenn Sie eine Datei auf Laufwerke oder Speicherkarten kopieren, die mit exFAT oder dem älteren FAT32 formatiert sind (wie es bei vielen Kameras und USB-Sticks der Fall ist), gehen die Zugriffsrechte verloren und die Datei ist für jedermann lesbar!

Der Zugriff auf Benutzerkonten sollte auf die zugehörigen Einzelpersonen beschränkt sein. Der Benutzer, der die Berechtigungen für die Konten einrichtet, sollte dem *Prinzip der minimalen Rechtegewährung* folgen. Konten sollten nur dazu berechtigt sein, genau auf jene Ressourcen zuzugreifen, die sie benötigen – und nicht mehr. Eine strenge Kontrolle der Benutzerkonten ist bei der Abwehr unberechtigter Zugriffe entscheidend. Die Deaktivierung nicht genutzter Konten ist ein wichtiger Teil dieser Strategie, aber eine gute Kontenverwaltung geht sehr viel weiter.

Mit Gruppen lässt sich die Komplexität gut steigern, ohne die administrative Last für die Netzwerkadministratoren zu erhöhen, weil alle Netzwerkbetriebssysteme Berechtigungen kombinieren. Wenn ein Benutzer Mitglied mehrerer Gruppen ist, welche Berechtigungen hat er dann für eine bestimmte Ressource? In allen Netzwerkbetriebssystemen werden Gruppenberechtigungen *kombiniert*, und daraus resultiert die sogenannte effektive Berechtigung, die Benutzer für den Zugriff auf eine Ressource besitzen. Dazu ein Beispiel. Wenn Rita Mitglied der Gruppe Verkauf ist, die zur Anzeige des Inhalts eines Ordners berechtigt ist, und außerdem Mitglied der Gruppe Manager mit Lese- und Ausführungsberechtigungen, dann darf sie sich nicht nur den Inhalt des Ordners anzeigen lassen, sondern verfügt *auch* über Lese- und Ausführungsberechtigungen.

Wichtig

Auf einem Dateiserver können Sie die Berechtigungen für Verzeichnisse verwenden, um den Zugriff auf sensible Informationen zu beschränken. Auf einem Mehrbenutzersystem lassen sich dadurch die Daten eines Benutzers vor dem Zugriff durch andere Benutzer schützen. Auch die zum Betriebssystem gehörende Software ist so davor geschützt, durch Programme oder Skripts kompromittiert zu werden, die ein Benutzer ausführt. Damit ist die Arbeit aber noch nicht erledigt! Jeder, der physischen Zugriff auf ein Laufwerk hat, kann die vorgegebenen Berechtigungen ignorieren. Verwenden Sie die vollständige Verschlüsselung des Laufwerks, um ruhende Daten (gespeicherte Daten, die nicht in Verwendung sind oder über das Netzwerk übertragen werden) zu schützen.

Achten Sie auf *vordefinierte* Benutzerkonten und -gruppen – sie können zu Sicherheitsrisiken für Ihr Netzwerk werden! In allen Netzwerkbetriebssystemen gibt es die vordefinierte Gruppe JEDER, die leicht genutzt werden kann, um sich Zugriff auf freigegebene Ressourcen zu erschleichen. Die Gruppe JEDER umfasst buchstäblich alle, die eine Verbindung zu dieser Ressource herstellen. Standardmäßig räumt Windows dieser Gruppe alle Berechtigungen ein, weshalb Sie diese sofort deaktivieren sollten! Auch das Gastbenutzerkonto kann eine Bedrohung darstellen. Es ist die einzige Möglichkeit, ohne Benutzernamen und Kennwort auf ein System zuzugreifen. Wenn es keinen wirklich guten Grund dafür gibt, ein Gastbenutzerkonto bereitzustellen, sollten Sie es deaktivieren.

Bei allen vordefinierten Gruppen (JEDER, GAST, BENUTZER) handelt es sich um weit gefasste, allgemeine Benutzergruppen. Verwenden Sie diese Gruppen allenfalls dann, wenn Sie wirklich allen Benutzern Zugriff auf eine Ressource gewähren wollen. Wenn Sie eine dieser vordefinierten Gruppen verwenden, achten Sie darauf, sie mit den richtigen Berechtigungen zu konfigurieren, damit Benutzer freigegebene Ressourcen nicht auf unerwünschte Weise manipulieren können!

Sicherheitsrichtlinien

Während sich über Berechtigungen steuern lässt, wie Benutzer auf freigegebene Ressourcen zugreifen, gibt es noch andere Funktionen, die Sie kontrollieren sollten, die über die reinen Zugriffsrechte auf Dateien und Ordner hinausgehen. Sollen Benutzer eines Windows-Systems beispielsweise auf die Eingabeaufforderung zugreifen dürfen? Sollen Benutzer Software installieren dürfen? Sollen sich Benutzer auf bestimmten Systemen nur zu bestimmten Tageszeiten anmelden können? Bei allen Netzwerkbetriebssystemen können Sie derartige und Hunderte weitere Sicherheitseinstellungen vornehmen. Unter Windows werden sie *Richtlinien* genannt. Ich stelle mir Richtlinien im Unterschied zu den eigentlichen Berechtigungen zur Steuerung von Ressourcenzugriffen gerne als Berechtigungen für Aktivitäten vor.

Eine Richtlinie wird normalerweise auf ein Benutzerkonto, einen Computer oder eine Gruppe angewendet. Betrachten wir dazu beispielhaft ein Netzwerk, das aus Windows-Systemen und einem Windows-Server besteht. Auf jedem Windows-Client gibt es ein eigenes lokales Programm, mit dem nur für das jeweilige System gültige Richtlinien definiert werden können. Abbildung 27.14 zeigt das Werkzeug, mit dem Sie lokale Richtlinien für die jeweiligen Systeme erstellen können (Lokale Sicherheitsrichtlinie) und mit dem Benutzerkonten beispielsweise das Recht zur lokalen Anmeldung entzogen werden kann.

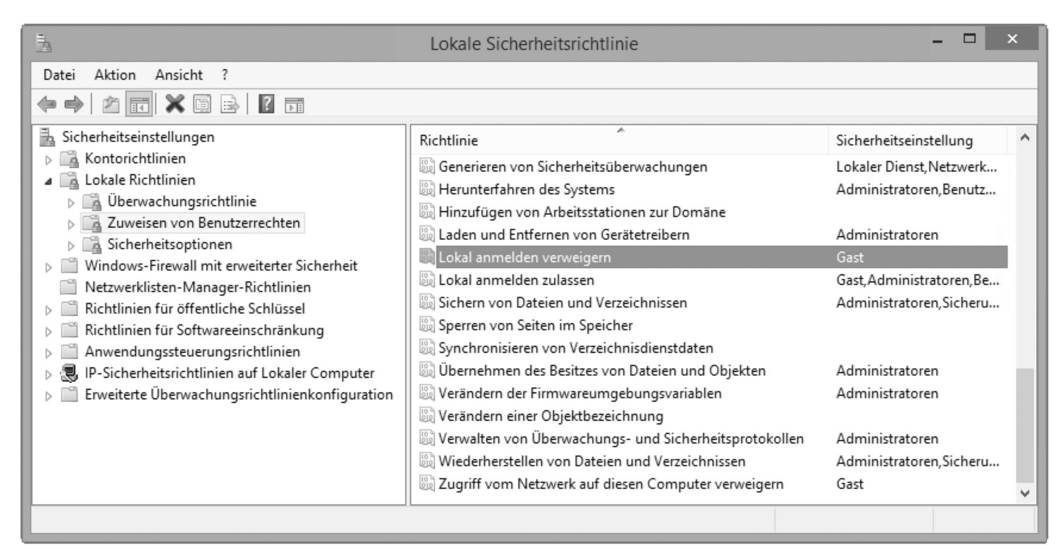


Abb. 27.14: Lokale Sicherheitsrichtlinie

Lokale Richtlinien eignen sich gut für einzelne Systeme, können aber sehr mühsam zu konfigurieren sein, wenn dieselben Einstellungen auf mehreren Rechnern in Ihrem Netzwerk angewendet werden sollen. Wenn Sie Sicherheitsrichtlinien für viele Benutzer definieren müssen, sollten Sie auf Windows Active Directory basierende Gruppenrichtlinien verwenden, die Sie aus Kapitel 19 kennen. Sie können Organisationseinheiten verwenden, um Benutzer und Geräte in einer Ordner-ähnlichen Hierarchie zu organisieren. Über Gruppenrichtlinien haben Sie viel mächtigere (Microsoft spricht von granularen) Möglichkeiten zur Verwaltung der Netzwerkclients einer solchen Einheit.

Wichtig

Änderungen an einer Gruppenrichtlinie sind möglicherweise nicht sofort auf allen Systemen wirksam. Windows aktualisiert die Gruppenrichtlinien, wenn das System gestartet wird oder wenn sich ein Benutzer anmeldet. Hin und wieder findet eine Aktualisierung auch im laufenden Betrieb statt, dennoch sind bestimmte Änderungen erst nach einem Neustart wirksam. Führen Sie auf der Kommandozeile den Befehl `gpupdate /force` aus, damit die Änderungen auf einem bestimmten Computer sofort wirksam werden.

Wollen Sie für alle Rechner innerhalb Ihrer Domäne einen einheitlichen Desktophintergrund festlegen? Mit Gruppenrichtlinien ist das möglich. Wollen Sie bestimmte Tools nur berechtigten Benutzern zugänglich machen? Auch das geht mit Gruppenrichtlinien. Wollen Sie den Zugang zum Internet kontrollieren, Heimverzeichnisse umleiten, Skripts ausführen, Software bereitstellen oder einfach nur dafür sorgen, dass unberechtigte Zugriffsversuche auf das Netzwerk schnell ins Nirwana führen? Gruppenrichtlinien sind die Lösung. Abbildung 27.15 zeigt eine Gruppenrichtlinie, die den Titel aller Instanzen des Internet Explorers für alle Benutzer eines lokalen Rechners in der Domäne ändert!

Dabei handelt es sich nur um ein primitives Beispiel für Einstellungen, die Sie mit Gruppenrichtlinien konfigurieren können. Es gibt Hunderte mehr oder weniger wichtige Einstellungen, mit denen Sie sich aber nicht unbedingt vertraut machen müssen. Gruppenrichtlinien sind ein wichtiges Thema in den Microsoft-Zertifizierungen aber für die CompTIA A+-Prüfungen müssen Sie nur das den Gruppenrichtlinien zugrunde liegende Konzept verstehen.

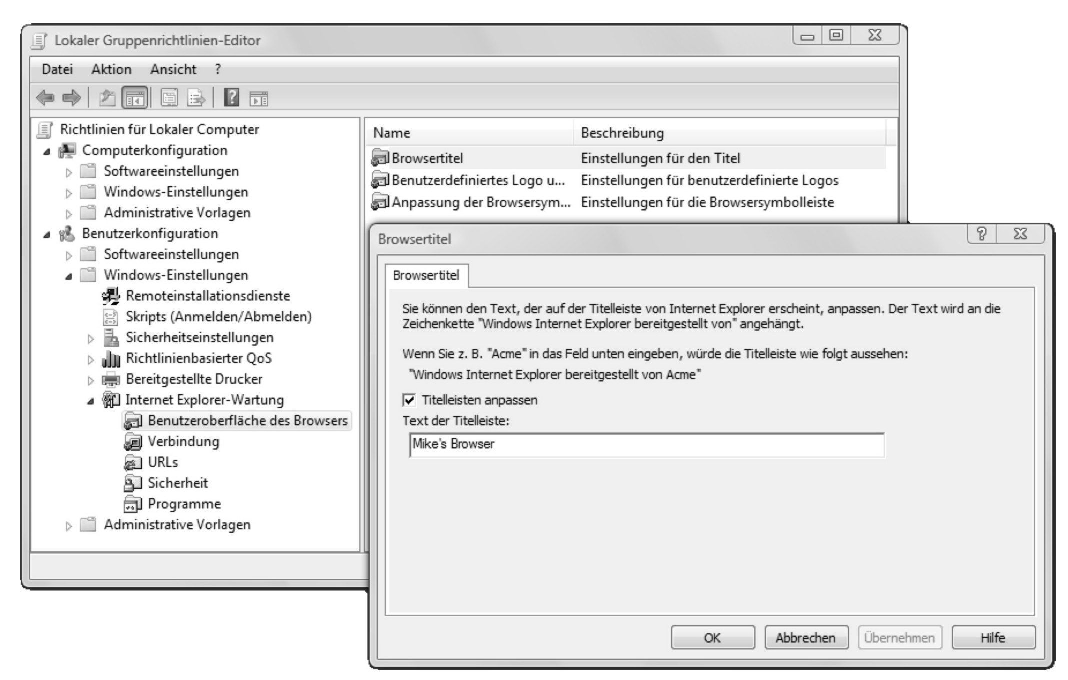


Abb. 27.15: Dank dieser Gruppenrichtlinie steht im Titel des Internet Explorers jetzt der von mir festgelegte Text!

Es ist zwar hier nicht möglich, alle Richtlinien aufzuführen, die Sie auf einem Windows-System aktivieren können, aber nachfolgend finden Sie einige der am häufigsten gebrauchten:

- **Die Bearbeitung der Registry verhindern**: Wenn Sie versuchen, die Registry zu bearbeiten, erhalten Sie eine Fehlermeldung.
- **Zugriff auf die Eingabeaufforderung untersagen**: Diese Richtlinie verhindert, dass Benutzer an die Eingabeaufforderung gelangen, indem der Befehl AUSFÜHREN und die Verknüpfung zur Eingabeaufforderung deaktiviert werden.
- **Lokale Anmeldung**: Diese Richtlinie definiert, wer sich lokal am System anmelden darf.
- **System herunterfahren**: Diese Richtlinie definiert, wer das System herunterfahren darf.
- **Mindestkennwortlänge**: Diese Richtlinie erzwingt eine Mindestlänge für das Kennwort.
- **Schwellenwert für die Kontensperre**: Diese Richtlinie legt fest, wie viele Anmeldeversuche eine Person höchstens unternehmen darf, bevor sie von dem Konto ausgesperrt wird.
- **Windows-Installer deaktivieren**: Diese Richtlinie verhindert, dass Benutzer Software installieren können.
- **Drucker-Browsing**: Diese Richtlinie ermöglicht den Benutzern, im Netzwerk nach Druckern zu suchen, damit sie nicht nur die ihnen zugewiesenen Drucker benutzen können.

Die CompTIA A+-Prüfungen erwarten von Ihnen zwar nicht, dass Sie wissen, wie diese Richtlinien in einem Netzwerk implementiert werden, aber Sie müssen doch wissen, dass es insbesondere in Windows-Netzwerken Richtlinien gibt, die Erstaunliches hinsichtlich der Kontrolle der Benutzer im System leisten können. Wenn Sie auf die Eingabeaufforderung eines Windows-Systems zuzugreifen versuchen und feststellen, dass der Befehl AUSFÜHREN deaktiviert ist, können Sie dafür eine Richtlinie und nicht den Computer verantwortlich machen!

Wichtig

Für die Verwaltung von Benutzerkonten gelten einige grundlegende Sicherheitsrichtlinien. Gewähren Sie nur die erforderlichen Zugriffsrechte, beschränken Sie den Zeitraum, in dem Anmeldungen erlaubt sind, sperren Sie Konten, wenn die Anmeldung zu oft fehlschlägt, und deaktivieren Sie die AutoRun/AutoPlay-Funktion des Betriebssystems. Zu guter Letzt sollten Sie immer die vorgegebenen Benutzernamen und Kennwörter ändern, sofern das möglich ist.

27.2.2 Datenklassifizierung und Konformität

In größeren Organisationen (z.B. Behörden) ist es äußerst nützlich, wenn Daten entsprechend ihrer Sensibilität kategorisiert und organisiert werden. Durch die *Datenklassifizierung* wird dafür gesorgt, dass die Computerhardware und die Software möglichst einheitlich bleiben. Darüber hinaus müssen innerhalb der Organisation viele rechtliche und interne Regeln ziemlich streng gehandhabt werden.

Wie die Daten klassifiziert werden, ist bei den einzelnen Unternehmen unterschiedlich. Bei einem verbreiteten Schema werden Dokumente als öffentlich, intern, streng vertraulich, streng geheim usw. klassifiziert. Wenn ein Klassifizierungsschema verwendet wird, wissen die Angestellten und auch die Techniker sehr schnell, wie mit bestimmten Dokumenten und Laufwerken verfahren werden muss. Ihre Vorgehensweise beim Recyceln des Computersystems eines auf einen neuen Rechner umgezogenen Mitarbeiters wird beispielsweise stark davon abhängig sein, ob sich auf dem Laufwerk nur als intern oder als streng geheim klassifizierte Daten befinden.

Konformität bedeutet kurzgefasst, dass sich die Mitglieder einer Organisation oder Mitarbeiter eines Unternehmens allen Regeln unterwerfen müssen, die für diese gelten. Gesetze und Statuten geben bestimmte Vorgehensweisen oder Verbote vor, an die sich Mitarbeiter am Arbeitsplatz halten müssen.

Aus der Perspektive des Technikers geht es beim verbreitetsten Konformitätsaspekt um die Software. Dabei gibt es Richtlinien, welche Software die Benutzer auf ihren Rechnern installieren dürfen oder wann und wie Sie ihnen mitteilen müssen, dass sie die neueste Programmversion nicht installieren dürfen, obwohl sie damit ihre Arbeit effizienter verrichten könnten, weil sich diese nicht auf der Liste der genehmigten Software befindet. Das kann zu einigen unangenehmen Auseinandersetzungen führen, die aber bei einem Techniker zum Beruf dazugehören.

Nicht genehmigte Software kann ein ernsthaftes Sicherheitsrisiko darstellen. Nicht-konforme Systeme sind ein klarer Verstoß gegen die Sicherheitsrichtlinien – beheben Sie solche Probleme umgehend.

Die der Konformität zugrunde liegenden Konzepte sollen nicht, wie es zunächst vielleicht aussehen mag, effizientes Arbeiten verhindern. Sie sollen vielmehr verhindern, dass Anwender ohne die notwendigen Fähigkeiten oder Kenntnisse potenziell schädliche oder die Systemstabilität gefährdende bzw. beeinträchtigende Programme oder Anwendungen installieren. Das sorgt dafür, dass die Zahl der Anrufe beim technischen Support gering bleibt und dass sich die Techniker auf wichtigere Probleme konzentrieren können.

Wichtig

Persönlich zuweisbare Informationen sind Daten, die es erlauben, eine bestimmte Person zu identifizieren. In der Prüfung können Fragen zur Klassifizierung von Daten vorkommen. Befragen Sie im Zweifel Ihre Vorgesetzten, ob es in Ihrem Unternehmen Richtlinien für den Umgang mit persönlich zuweisbaren Daten gibt.

27.2.3 Lizenzierung

Bei der Lizenzierung von Software gibt es viele Fallstricke, die schnell dazu führen können, dass ein Benutzer oder ein Techniker gegen eine der gültigen Regeln verstößt. Wie bei anderen Werken mit

einer sogenannten *Schöpfungshöhe*, besitzen Programmierer ein Urheberrecht für die von ihnen geschriebene Software. Der Urheber entscheidet, wie die Software lizenziert wird. Es gibt kommerzielle und nicht kommerzielle sowie personengebundene oder firmenweite Lizenzen. Der Quellcode kann öffentlich zugänglich sein – oder auch nicht. Bei all diesen Möglichkeiten gibt es darüber hinaus weitere Varianten, die Sache ist tatsächlich ziemlich kompliziert. Sehen wir uns also die verschiedenen Lizenzen der Reihe nach an.

Kommerzielle Lizenzierung

Wenn Software unter einer kommerziellen Lizenz veröffentlicht wird, sind Sie rechtlich dazu verpflichtet, Geld für deren Nutzung zu bezahlen – allerdings gibt es hier viele Varianten. Früher war es üblich, dass man ein Programm erwarb und es dann unbefristet nutzen durfte. Man durfte es weiterverkaufen oder verschenken. Man erwarb entweder für jede Kopie eine eigene Lizenz oder eine Firmenlizenz für mehrere Benutzer.

Heute ist es nicht mehr so einfach. Für Microsoft Office gibt es beispielsweise zeitlich befristete Lizenzen. Sie dürfen die Software nutzen, solange Sie eine monatliche oder jährliche Lizenzgebühr entrichten. Die persönliche Lizenz gestattet es Ihnen, die Software mit mehreren anderen Personen auf verschiedenen privaten Computern gemeinsam zu verwenden.

Die *Endbenutzer-Lizenzvereinbarung* (*EULA*, *End User License Agreement*), der Sie sich unterwerfen, wenn Sie Software installieren, verpflichtet Sie dazu, sich bei der Nutzung und Weitergabe an die vom Urheber festgelegten Regeln und Vorschriften zu halten. Sie stimmen also der EULA von Microsoft Office zu und kommen damit überein, keine illegalen Kopien zu erstellen und die Software nur auf die von Microsoft zugelassene Weise zu nutzen.

Durch verschiedene Formen einer *digitalen Rechteverwaltung* (*DRM*, *Digital Rights Management*) kann erzwungen werden, wie sich kommerzielle Software nutzen lässt. Bei vielen Programmen ist eine Aktivierung über das Internet oder ein spezielles Benutzerkonto beim Urheberrechtsinhaber erforderlich. Um Software von Adobe zu verwenden, wie etwa Photoshop, benötigen Sie z.B. ein Adobe-Benutzerkonto.

Nicht-kommerzielle Lizenzierung

Manche Entwickler möchten aus ethischen oder philosophischen Gründen, dass ihre Software für bestimmte Zwecke oder generell kostenlos zu haben ist. Beispielsweise stellte Linus Torvalds das Betriebssystem Linux kostenlos bereit, nachdem er es entwickelt hatte. Die Bildbearbeitungssoftware GIMP steht ebenfalls kostenlos zur Verfügung.

Bei der nicht-kommerziellen Lizenzierung gibt es verschiedene Varianten. Viele dieser Programme sind nur für den persönlichen Gebrauch kostenlos. Wenn Sie beispielsweise das ausgezeichnete Fernsteuerungsprogramm *Team Viewer* auch beruflich nutzen möchten, müssen Sie eine kommerzielle Lizenz erwerben. Wenn Sie sich mit Ihrem privaten Laptop am heimischen Computer anmelden, ist die Nutzung von Team Viewer hingegen umsonst.

Open Source vs. Closed Source

Bei der Nutzung und Lizenzierung von Software gibt es hinsichtlich der Nutzung des Quellcodes einer Anwendung große Unterschiede. Open-Source-Lizenzen gestatten es im Allgemeinen, den ursprünglichen Code zu modifizieren. Bei manchen Lizenzmodellen sind Sie allerdings dazu verpflichtet, den modifizierten Code kostenlos zum Herunterladen bereitzustellen. Handelt es sich um Closed Source, legt die Lizenz fest, dass Sie keinen Einblick in den Quellcode der Anwendung bekommen und diese auch nicht zum Teil eines anderen Softwareprodukts machen dürfen.

In den Lernzielen der CompTIA A+-Prüfung 1002 ist zwar »Open Source vs. kommerzielle Lizenz« aufgeführt, tatsächlich existiert eine solche Unterscheidung aber gar nicht. Es gibt jede Menge Open-Source-Programme, für die Lizenzgebühren erhoben werden, beispielsweise für die Serverversionen von Linux. Umgekehrt gehören auch viele kostenlose Programme in die Kategorie Closed Source.

Aus Sicht des Technikers ist es wichtig, die vom Unternehmen erworbenen Lizenzen genau zu kennen und dafür zu sorgen, dass sich das Unternehmen an die Lizenzbedingungen hält. Illegale Software einzusetzen, mehr Lizenzen zu nutzen, als durch die Lizenzvereinbarung erlaubt ist, oder Privatlizenzen in einem kommerziellen Unternehmen zu verwenden, kommt einem Diebstahl gleich. Dabei spielt es keine Rolle, wie leicht das in der Praxis möglich ist.

27.2.4 Reaktion auf Zwischenfälle

Organisationen benötigen Richtlinien und Verfahren, um mit negativen Ereignissen umzugehen, die Auswirkungen auf das Netzwerk und die Systeme haben. Je größer eine Organisation ist, desto detaillierter müssen die Reaktionen auf derartige Zwischenfälle ausgearbeitet sein, sowohl für das beteiligte Team als auch für die Vorgehensweise beim Eintreten aller Eventualitäten. Das ist ein äußerst umfangreiches Thema, dem wir bei fortgeschritteneren Zertifizierungen, wie CompTIA Security+, viel Zeit widmen. Als CompTIA A+-Techniker müssen Sie verstehen, welche Rolle Sie einnehmen und was Sie tun sollten (und was Sie unbedingt unterlassen sollten), wenn ein Zwischenfall eintritt. In diesem Abschnitt erkunden wir die erste Reaktion, das Erkennen und Berichten über Zwischenfälle sowie den Umgang mit Beweismitteln.

Erste Maßnahmen

Wenn Sie dem für Maßnahmen bei Zwischenfällen zuständigen Team angehören, ist in einem entsprechenden Plan festgelegt, was Sie beim Eintreten eines Zwischenfalls als Erstes unternehmen müssen. Höchstwahrscheinlich muss Ihr Team den betroffenen Bereich zunächst einmal absichern, wenn es zu einem Vorfall kommt. Anschließend müssen Sie feststellen, wie weitreichend der Zwischenfall ist (ob nur ein System oder eine ganze Benutzergruppe betroffen ist usw.) und ermitteln, wie ernst das Problem ist und welche Auswirkungen es auf das Unternehmen hat.

Die Absicherung des betroffenen Bereichs kann physischer Art sein (niemand darf den Bereich betreten oder verlassen) oder andere Maßnahmen umfassen (kein ein- oder ausgehender Netzwerkdatenverkehr im betroffenen Bereich). Um das Ausmaß des Vorfalls zu ermitteln, können Sie Benutzer befragen, Protokolldateien überprüfen und so weiter. Um die möglichen Auswirkungen, mit denen sich die Organisation konfrontiert sieht, kümmern sich die Netzwerkfachleute und das Sicherheitspersonal.

Erkennung und Bericht

Letztendlich müssen alle Sicherheitsprobleme einem Netzwerkadministrator oder Techniker gemeldet werden, damit dieser geeignete Maßnahmen zu deren Behebung ergreifen kann. Unter Windows können Sie die Ereignisanzeige nutzen, um sich vom Betriebssystem über Probleme informieren zu lassen. Sie können dann Ihre Arbeit erledigen und die Probleme melden.

Überwachung Im Abschnitt SICHERHEIT in der Ereignisanzeige wird standardmäßig nicht viel angezeigt. Um das volle Potenzial der Ereignisanzeige nutzen zu können, müssen Sie die Überwachung einrichten. Die Überwachung bedeutet in Hinblick auf die Sicherheit, dass Sie dafür sorgen, dass Windows bei bestimmten Ereignissen Einträge in das Sicherheitsprotokoll vornimmt. Dabei kann z.B. überwacht werden, wann sich Benutzer anmelden (Ereignisüberwachung) oder versuchen, auf eine bestimmte Datei oder einen Ordner zuzugreifen (Objektzugriffsüberwachung). Abbildung 27.16 zeigt die Ereignisanzeige bei der Überwachung von Anmelde- und Abmeldeereignissen.

Die CompTIA A+-Zertifizierungsprüfung testet nicht, ob Sie brillante Überwachungsstrategien für Ihr Büro einrichten können, denn das zählt zu den Aufgaben der Netzwerkadministratoren. Sie müssen nur wissen, was bei der Überwachung passiert und wie Sie diese zur Unterstützung des Netzwerkadministrators aktivieren oder deaktivieren können. Um die Überwachung lokal zu aktivieren, rufen Sie in der Systemsteuerung erst VERWALTUNG und dann das Applet LOKALE SICHERHEITSRICHTLINIE auf. Markieren Sie dann unter dem Eintrag LOKALE RICHTLINIEN die Option ÜBERWACHUNGSRICHTLINIE. Doppelklicken Sie auf eine der Richtlinienoptionen und markieren Sie die gewünschten Kontrollkästchen. Abbildung 27.17 zeigt das Dialogfeld zur Überwachung der Objektzugriffe.

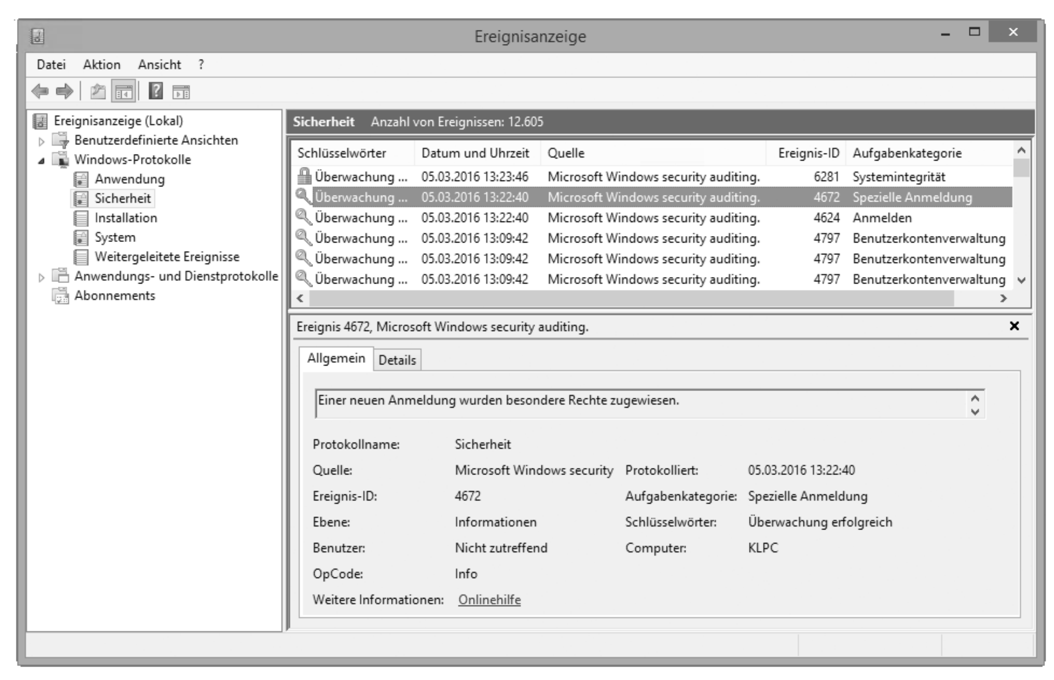


Abb. 27.16: Ereignisanzeige mit Sicherheitshinweisen

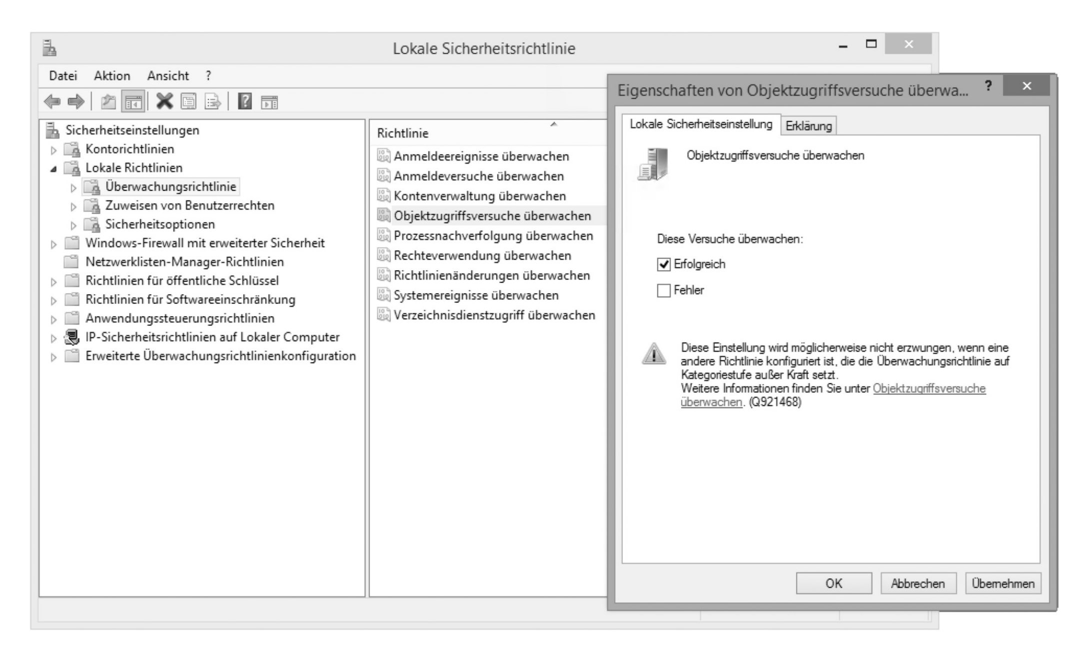


Abb. 27.17: Überwachung von Objektzugriffsversuchen mit dem Fenster LOKALE SICHERHEITSRICHTLINIE im Hintergrund

Hinweis

Die Ereignisanzeige speichert ihre Protokolldateien im Ordner `%SystemRoot%\System32\Config`.

Zwischenfallberichte Wenn Sie Daten über ein bestimmtes System gesammelt oder ein Computer- oder Netzwerkproblem behoben haben, müssen Sie darüber meist Ihrem Vorgesetzten berichten. Man spricht auch von *Zwischenfallberichten*. Viele Unternehmen haben vorgefertigte Formulare, die Sie einfach ausfüllen und weiterleiten. Andere gehen weniger formal vor. Unabhängig von der Verfahrensweise müssen Sie diese Aufgabe jedoch erledigen!

Die Zwischenfallberichte haben verschiedene Vorteile. Erstens protokollieren Sie damit die von Ihnen verrichteten Arbeiten. Zweitens stellen sie Informationen bereit, die zusammen mit anderen möglicherweise Muster erkennen lassen und auf schwerwiegendere Probleme hinweisen können. Ein scheinbar unwichtiger Sicherheitsüberwachungsbericht könnte z.B. zu vielen ganz ähnlichen Ereignissen an mehreren Stellen im Gebäude passen und damit darauf hindeuten, dass es sich nicht um eine zufällige Störung, sondern um eine koordinierte, zielgerichtete Ursache handelt.

Umgang mit Beweismitteln

Es bleibt nicht aus, dass Sie sich als Techniker mit Leuten befassen müssen, die Firmencomputer auf unerlaubte Weise benutzen. In den meisten Fällen werden Sie nicht behelligt und haben nichts weiter zu tun. Es kommt dennoch vor, dass wirklich üble Machenschaften auf von Ihnen betreuten Systemen stattfinden, und wenn Sie der erste Techniker vor Ort sind, wird man sich an Sie wenden, damit etwas unternommen wird.

Wichtig

Rechnen Sie in der CompTIA A+-Prüfung 220-1002 mit Fragen zum Umgang mit Beweismitteln.

Techniker sollten persönliche Informationen ignorieren, egal ob sich diese direkt auf dem System oder in dessen Umgebung befinden. Wie in Kapitel 1 erläutert, sollten Sie alles, was Ihnen anvertraut wird, und alles, was Sie zu Gesicht bekommen, vertraulich behandeln und nicht an andere Kunden, Kollegen oder Vorgesetzte weitergeben. Eine einfache Regel hierfür lautet: »Wenn es sich nicht um eine Straftat handelt oder eine unmittelbare Gefahr für Leib und Leben besteht, dann haben Sie auch nichts gesehen.« Das umfasst sämtliche vertraulichen Materialien Ihrer Kunden. Versuchen Sie, sich nur mit den Dingen zu befassen, die unmittelbar mit Ihrer Aufgabe zu tun haben. (Das ist natürlich manchmal unmöglich, aber Sie müssen Ihr Schicksal ja nicht auf die Probe stellen.) Wenn Sie beispielsweise an einem Drucker auf einen Ausdruck warten und der Drucker plötzlich die Lohnabrechnungen ausgibt, schieben Sie das Papier zur Seite und tun Sie so, als ob Sie nichts gesehen hätten.

Und was ist mit den wirklich beängstigenden Dingen? Offensichtliche Industriespionage? Kinderpornografie? Leute, die unbefugt persönliche Daten weitergeben? Hacker? In solchen Fällen müssen Sie erste Maßnahmen ergreifen. Betrachten wir die von der CompTIA aufgeführten Punkte.

Verbotene Handlungen und Inhalte erkennen Benutzen Sie Ihren gesunden Menschenverstand, aber bedenken Sie dabei, dass in den meisten Unternehmen klare Nutzungsvereinbarungen gelten, die von den Benutzern schriftlich anerkannt werden müssen. In der Nutzungsrichtlinie ist festgelegt, zu welchen Zwecken die Geräte des Unternehmens eingesetzt werden dürfen. Dabei geht es nicht nur um auf der Hand liegende Dinge wie privates Surfen im Internet, sondern neben Computern auch um Telefon, Drucker und sogar das Netzwerk selbst. Auch der Umgang mit Kennwörtern, E-Mail und vieles andere mehr ist in der Nutzungsvereinbarung festgeschrieben.

Berichterstattung Für gewöhnlich werden Sie verbotene Handlungen oder Inhalte direkt Ihrem Vorgesetzten melden. Vielleicht gibt es in Ihrem Unternehmen aber auch einen Sicherheitsbeauftragten, der für solche Fälle zuständig ist. Sprechen Sie jedoch *nicht* mit der Person, die den Regelverstoß begangen hat, bevor Ihr Vorgesetzter dies genehmigt.

Beweissicherung Wenn es sich um eine ernste Angelegenheit handelt, kann es dazu kommen, dass ein Computer (oder ein anderes Gerät) zu einem Beweisstück wird. In derartigen Fällen kann es von Bedeutung sein, wo sich das Gerät befand und wer es wann benutzt hat. Sie müssen daher eine Art Fahrtenbuch für den Computer erstellen, das die Verwahrungskette belegt, also ein Dokument, aus dem hervorgeht, wer das Gerät wann verwendet hat. Hoffentlich steht Ihnen dann ein rechtlicher Beistand zur Verfügung, aber hier einige der üblichen Vorgehensweisen:

1. Machen Sie das System unzugänglich. Fahren Sie den Computer herunter und lagern Sie ihn an einem Ort, an dem niemand darauf zugreifen kann.
2. Dokumentieren Sie den Zeitpunkt, an dem Sie das Gerät in Besitz genommen haben, und alle daran durchgeführten Handlungen: dass Sie das System heruntergefahren haben, es vom Netzwerk und Stromnetz getrennt haben, wo Sie es verstaut haben usw. Zerbrechen Sie sich nicht den Kopf über jedes einzelne Detail, aber der Aufbewahrungsort ist unverzichtbar.
3. Falls jemand anderes das Gerät in Besitz nimmt, sollten Sie das ebenfalls dokumentieren.

27.3 Netzwerksicherheit

Netzwerke werden auch von außen bedroht, daher werden in diesem Abschnitt Aspekte untersucht, die Angriffe aus dem Internet, Firewalls und drahtlose Netzwerke betreffen. Diese Dinge gehören zu den täglichen Aufgaben eines CompTIA A+-Technikers, sodass Sie die Konzepte und Vorgehensweisen verstehen müssen, um sie richtig implementieren zu können.

27.3.1 Schadsoftware

Das Internet ist deshalb so interessant, weil es am heimischen Sessel bequemen Zugang zu weltweiten Ressourcen bietet. Dabei werden aber Daten in beiden Richtungen ausgetauscht, sodass Menschen weltweit theoretisch ebenfalls von ihren verwunschenen Schlupfwinkeln aus auf Ihren Computer zugreifen können. Im Internet gibt es eine Menge *Schadsoftware* (*Malware*), die auch in diesem Moment Ihre Systeme zu infizieren versucht.

Bei Malware handelt es sich um Programme oder Code (Makros, Skripts usw.), die in Rechner einbrechen oder Chaos darauf anrichten sollen. Die gängigsten Varianten sind Viren, Würmer, Ransomware, Spyware, Trojaner, Keylogger und Rootkits. Sehen wir uns also die verschiedenen Malware-Typen und deren Funktionsweise an, um zu verstehen, wie sie überhaupt auf den Rechner gelangen können.

Arten von Schadsoftware

Schon seit den 1980er-Jahren werden PC-Benutzer von Schadsoftware geplagt, die sich im Laufe der Jahre zu unterschiedlichen Arten weiterentwickelt hat. Von den klassischen Bootsektor-Viren der 90er bis hin zu den aktuellen Bedrohungen durch Malware, die Ihre Festplatte verschlüsselt (»CryptoLocker«) und Infektionen, die durch den bloßen Aufruf einer Webseite zustande kommen: Malware ist eine ständige, sich permanent ändernde Gefahr für Ihre Benutzer und Ihre Daten. Sie müssen die verschiedenen Malware-Typen verstehen, um sich und Ihre Benutzer erfolgreich dagegen verteidigen zu können.

Viren Ein *Virus* ist ein Programm, das zwei Aufgaben erledigt: Replikation und Aktivierung. Bei der *Replikation* kopiert sich das Virus selbst, oft in Form von Code, der im Bootsektor eines Laufwerks abgelegt oder am Ende ausführbarer Programme angehängt wird. Bei der *Aktivierung* wird das Virus tätig und löscht beispielsweise Dateien oder stiehlt persönliche Daten. Viren replizieren sich nur auf andere Laufwerke, nicht direkt über das Netzwerk. Zur Verbreitung von Viren ist es erforderlich, dass der Benutzer tätig wird (Programm öffnen, Laufwerke anschließen usw.).

Würmer *Würmer* ähneln Viren, sie replizieren sich jedoch über Rechnernetzwerke oder Hardware, wie etwa Zubehör mit Thunderbolt-Anschlüssen. Anders als ein Virus ist ein Wurm nicht darauf ange-

wiesen, dass Wechseldatenträger verwendet werden, um sich auszubreiten. Falls der infizierte Rechner am Netzwerk angeschlossen ist, beginnt ein Wurm sofort damit, Kopien seiner selbst an andere Rechner, die er im Netzwerk findet, zu versenden.

Trojaner Ein *Trojaner* ist ein eigenständiges Programm, das vorgibt, eine bestimmte Aufgabe zu erledigen, in Wahrheit aber – wie die Soldaten im Inneren des antiken Trojanischen Pferdes – Böses im Schilde führt. Trojaner geben sich oft als Spiele, wie Poker, oder ironischerweise als kostenlose Sicherheitstools aus, der Fantasie sind hier aber kaum Grenzen gesetzt. Trojaner können die Kontrolle über den Computer übernehmen und sind ebenso hartnäckig wie Viren und Würmer, vervielfältigen sich im Gegensatz zu diesen jedoch nicht.

Keylogger *Keylogger* tun genau das, was Sie sich vorstellen: Sie zeichnen die Tastatureingaben des Benutzers auf und stellen sie dem Programmierer der Schadsoftware bereit. Die Aufzeichnung von Tastatureingaben ist oft auch Bestandteil anderer Schadsoftware. Keylogger müssen nicht notwendigerweise Schadsoftware sein – viele Kindersicherungen nutzen sie ebenfalls.

Rootkits Damit Viren oder Trojaner dauerhaft arbeiten können, müssen sie unentdeckt bleiben. Die Leute sind sich der Gefahr von Schadsoftware zunehmend bewusst und Anti-Malware-Software macht es immer schwieriger, Schadsoftware auf einem Computer zu verstecken. Ein *Rootkit* ist ein Programm, das sich grundlegende Funktionen des Betriebssystems zunutze macht, um sich vor Anti-Malware-Software zu verstecken, was auch gelingt, wenn nicht außerordentlich aggressive und spezialisierte Anti-Malware eingesetzt wird. Noch schlimmer ist allerdings, dass ein Rootkit definitionsgemäß Root-Rechte besitzt. Mit Rootkits lassen sich Betriebssystem, Hypervisor und sogar Firmware umgehen (davon sind auch Festplatten und Zubehör betroffen ... Meine Güte!).

Vor einigen Jahren tauchte ein berühmt-berüchtigtes Rootkit auf, das Sony beim Versuch einsetzte, Musik-CDs vor Piraterie zu schützen. Für den Mediengiganten Sony war es eine peinliche Angelegenheit, dass dieses Rootkit, das beim Abspielen einer Musik-CD installiert wurde, eine Hintertür öffnete, die sich für bösartige Zwecke missbrauchen ließ.

Verhaltensweise von Schadsoftware

Schön und gut, wenn man die verschiedenen Arten von Schadsoftware kennt, aber wirklich von Bedeutung ist eigentlich nur, wie »schädlich« eine Schadsoftware tatsächlich ist, wenn sie auf einem System Amok läuft. Sehen wir uns dazu zunächst einmal einen alten Bekannten an: Spyware.

Spyware Spyware ist Schadsoftware, die im Allgemeinen ohne Ihr Wissen installiert wird und die Ressourcen Ihres Computers zur Ausführung verteilter Anwendungen, zur Aufzeichnung von Tastatureingaben oder Schlimmeres nutzen kann. Klassische *Spyware* gelangt oft zusammen mit eigentlich rechtmäßiger Software auf ein System – Software, die reibungslos funktioniert und dem Benutzer irgendwelche Vorteile verspricht. Welche Art Vorteile? Im Jahre 2005 stellte die Firma Movieland (ebenfalls bekannt unter Movieland.com und Popcorn.net) einen »praktischen« Dienst zum Herunterladen von Spielfilmen vor. Das klang verlockend und viele Leute installierten sich den Dienst. Den Benutzern wurde allerdings nicht mitgeteilt, dass durch die Installation der erforderlichen Software automatisch ein Vertrag mit dreitägiger Testphase abgeschlossen wurde. Wenn man nicht vor Ablauf der Testphase kündigte, erschien ein Pop-up, das zur Zahlung für den Dienst aufforderte, den wissentlich niemand abonniert hatte. Das Beste kommt noch: Die Anwendung ließ sich nicht vollständig deinstallieren. Das Programm zum Deinstallieren leitete die Benutzer auf eine Webseite um, die erneut zur Zahlung aufforderte. (Movieland wurde 2007 aufgelöst.)

Ein weiteres klassisches Beispiel sehen Sie in Abbildung 27.18: Der Benutzer wird aufgefordert, der Gator Corporation (einem seinerzeit wohlbekannten Spyware-Produzenten) zu vertrauen. Da es sich schnell herumsprach, dass man Gator besser nicht vertraut, lehnte jeder vernünftige Benutzer das natürlich ab, und Gator verschwand kurze Zeit später wieder von der Bildfläche.

2005 war Movieland der Bösewicht. Und wer treibt heutzutage sein Unwesen mit Spyware? Leider lässt sich das nicht so einfach sagen, weil man es einfach noch nicht weiß. Heutzutage wird Ihnen Spyware vermutlich am ehesten in der CompTIA A+-Zertifizierungsprüfung 1002 begegnen.

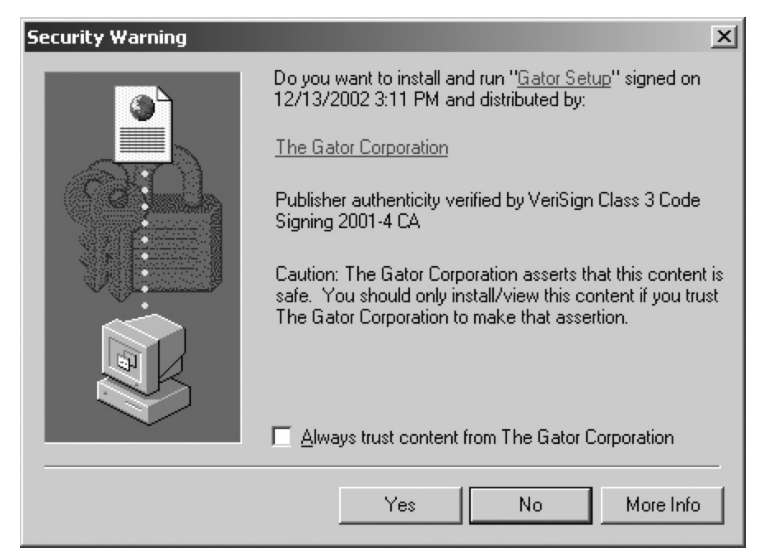


Abb. 27.18: Die Installationsbestätigung der Gator Corporation

Ransomware So schlimm Spyware auch ist, Sie kommen jedenfalls noch an Ihre Daten heran. *Ransomware* hingegen verschlüsselt alle Daten, auf die sie zugreifen kann. Viele Versionen dieser Erpressungstrojaner sind sogar in der Lage, die auf Netzlaufwerken befindlichen Daten zu verschlüsseln!

Nachdem alle Daten verschlüsselt worden sind, erscheint eine Meldung der Ransomware, in der Sie aufgefordert werden, für die Entschlüsselung Ihrer Daten Geld zu bezahlen. (Nicht selten werden auch Bitcoins verlangt). Um eine möglichst schnelle Zahlung zu erzwingen, wird außerdem ein rückwärtslaufender Zähler präsentiert und damit gedroht, den Code zum Entschlüsseln Ihrer Daten zu löschen, wenn der Zähler bei null ankommt. Sie hätten dann nur noch eine Festplatte voller unbrauchbarer Daten.

Wichtig

Die verschiedenen Arten von Schadsoftware (Viren, Würmer, Trojaner, Keylogger, Rootkits, Spyware und Ransomware) sollten Sie kennen.

Ein Netz voller Zombies Eine weitere Art von Schadsoftware, auf die ich kurz eingehen möchte, ist ein Botnet (»Bot« wie in Ro*bot*er). Bei einem Botnet handelt es sich nicht um eine einzelne Schadsoftware, sondern um ein ganzes Netz von Rechnern (»Zombies«), die damit infiziert sind. Dieses Netz steht unter der Kontrolle einer einzelnen Person oder Gruppe, und größere Botnets können mehrere Millionen Zombie-Rechner umfassen.

Ein Netz mit so vielen Computern bedeutet, dass dem Betreiber eines Botnets Rechenleistung und Netzwerkbandbreite in großem Umfang zur Verfügung stehen. Zumeist werden Botnets zum Versenden von Spam eingesetzt. Haben Sie sich schon einmal gefragt, wie sich Spammer die Kosten für die enorme Bandbreite leisten können, die sie brauchen? Sie zahlen gar nicht dafür! Sie missbrauchen die Bandbreite der Millionen auf der ganzen Welt verteilten Zombie-Rechner, von Omas E-Mail-Rechner bis hin zu gehackten Webservern.

Der Versand von Spam ist jedoch nicht der einzige Zweck von Botnets. Die kriminellen Betreiber nutzen die gesammelte Bandbreite auch dazu, die Rechner von Unternehmen und Organisationen durch sinnlose Anfragen lahmzulegen und verlangen dann ein Lösegeld, um den Angriff wieder abzublasen.

Angriffsmethoden und Herkunft von Schadsoftware

So schlimm diese ganze Malware auch ist, sie findet doch nicht von ganz allein ihren Weg auf einen Rechner. Dazu ist vielmehr das erforderlich, was Sicherheitsexperten als einen *Angriffsvektor* bezeichnen – die Methode, die es einer Schadsoftware ermöglicht, auf einen Computer zu gelangen und ihn zu infizieren. Als guter Techniker müssen Sie wissen, wo die Schwachstellen liegen, um gewährleisten zu können, dass Ihre Computer geschützt sind.

Wie so oft, führen viele Wege nach Rom, und es gibt eine ganze Reihe von Möglichkeiten, wie Schadsoftware auf ein System gelangen kann, von den ersten Bootsektor-Viren auf Disketten bis hin zu den heutigen Würmern und Infektionen, die durch den bloßen Aufruf einer Webseite zustande kommen.

Zero-Day-Angriffe Ein *Zero-Day-Angriff* beschreibt das Ausnutzen einer Sicherheitsschwachstelle, die dem Softwareentwickler noch gar nicht bekannt war. Der Name stammt daher, dass der Entwickler der fehlerhaften Software exakt null Tage Zeit hatte, die Schwachstelle zu beheben. Microsoft, Apple und andere Softwareentwickler stellen regelmäßig Patches bereits, sobald derartige Fehler entdeckt werden.

Spoofing Wenn Datenpakete falsche Informationen enthalten, um einen anderen Absender oder eine andere Herkunft vorzutäuschen, bezeichnet man das als *Spoofing*. Alle über ein Netzwerk versendeten Daten können auf diese Weise manipuliert worden sein. Ein paar Beispiele für gefälschte Daten:

- MAC- oder IP-Adresse, um eine andere Herkunft eines Datenpakets vorzutäuschen
- E-Mail-Adresse, um einen anderen Absender einer E-Mail vorzutäuschen
- Internetadressen, um eine andere Website vorzutäuschen
- Benutzernamen, um vorzutäuschen, dass sich ein bestimmter Benutzer anmeldet, obwohl es sich in Wahrheit um jemand völlig anderen handelt

Das Spoofing an sich stellt weniger eine Gefahr dar, dient aber oft dazu, eine Bedrohung erst zu schaffen. Wenn Sie beispielsweise eine E-Mail mit meiner E-Mail-Adresse als Absender versehen, ist das für sich genommen noch nicht bedrohlich. Wenn Sie meine E-Mail-Adresse jedoch verwenden, um sich für mich auszugeben und meine Mitarbeiter in meinem Namen dazu auffordern, ihre Benutzernamen und Kennwörter für die Anmeldung im Netzwerk zu senden, stellt das zweifelsohne eine Bedrohung dar – wäre allerdings auch Zeitverschwendung, denn meine Mitarbeiter würden mir *niemals* ihre Zugangsdaten verraten.

Man-in-the-middle-Angriff Bei einem *Man-in-the-middle-Angriff* zapft ein Angreifer heimlich den Datenverkehr zwischen zwei Systemen an, von denen man glaubt, dass sie nur untereinander kommunizieren. Er kann die übertragenen Daten mitlesen und sogar manipuliert weiterleiten. Bei einem klassischen Man-in-the-middle-Angriff könnte man in einem drahtlosen Netzwerk einen Laptop mit spezieller Software als Zugangspunkt ausgeben. Der gesamte Datenverkehr wäre zugänglich und man könnte Kennwörter und andere vertrauliche Information in Erfahrung bringen.

Session Hijacking Ähnlich wie beim Man-in-the-middle-Angriff wird beim *Session Hijacking* die Verbindung zwischen zwei Systemen angezapft, die Verbindung bzw. die Sitzung ist jedoch authentifiziert. Durch die Übernahme dieser Sitzung erlangt der Angreifer dieselben Zugriffsrechte wie der rechtmäßig authentifizierte Benutzer. Anders als beim Man-in-the-middle-Angriff geht es hier weniger um das Belauschen der Verbindung, sondern vornehmlich um die Zugangsdaten.

Brute Force Die CompTIA beschreibt *Brute Force* als eine Bedrohung, eigentlich handelt es sich jedoch eher um eine Angriffsmethode, bei der ein Angreifer viele oder alle möglichen Werte durchprobiert, etwa für Benutzernamen oder Kennwort. Meistens ist mit dem Begriff der Versuch gemeint, ein Kennwort zu knacken, er kann sich jedoch auch auf andere Angriffe beziehen, beispielsweise auf die Suche nach offenen Ports, Netzwerk-IDs, Benutzernamen usw. Praktisch jeder Versuch, den nicht offensichtlichen oder verborgenen Inhalt eines Datenfelds zu erraten, wird als Brute-Force-Angriff bezeichnet.

Die CompTIA listet zwei weitere Werkzeuge auf, die Angreifer zum Knacken von Kennwörtern verwenden: Wörterbücher und Rainbow Tables (Regenbogentabellen). Ein *Wörterbuchangriff* ist eine

besondere Form eines Brute-Force-Angriffs, bei dem sämtliche in einem Wörterbuch enthaltenen Wörter durchprobiert werden. Denken Sie dabei nicht nur an Nachschlagewerke wie den Duden – ein für Wörterbuchangriffe genutztes Wörterbuch könnte sämtliche Kennwörter enthalten, die jemals online veröffentlicht wurden.

Bevor wir uns mit Rainbow Tables befassen, müssen wir einen Blick auf verloren gegangene Kennwörter werfen. Eine (furchtbare!) Möglichkeit, Benutzer zu authentifizieren, besteht darin, ihre Kennwörter in einer Datenbank zu speichern und diese bei der Anmeldung abzufragen. Hacker *lieben* es, solche Datenbanken zu stehlen, weil sie die Benutzernamen und Kennwörter bei verbreiteten Diensten ausprobieren können. Zudem verwenden sie die Kennwörter, um ihre Wörterbücher zum Erraten von Kennwörtern zu verbessern.

Um diese Bedrohung zu vermeiden, verwenden Authentifizierungssysteme einen speziellen Wert, der anhand des Kennworts berechnet wird, einen sogenannten *Hash*. Wenn ein Benutzer sich anmeldet, berechnet das System diesen Wert erneut und vergleicht ihn mit dem hinterlegten. Wenn ein Hacker eine solche Datenbank stiehlt, bekommt er nur einen Haufen Benutzernamen und Hashes zu sehen. Hashes sind insofern etwas Besonderes, weil ihre Berechnung irreversibel ist, also nicht umkehrbar. Es gibt nur eine Möglichkeit, herauszufinden, welches Kennwort einen bestimmten Hash erzeugt, nämlich ein Kennwort zu raten, den Wert erneut zu berechnen und zu überprüfen, ob die Hashwerte übereinstimmen.

Die Angreifer haben daraufhin große Tabellen zum Nachschlagen erstellt, sogenannte *Hashtabellen*, die Kennwörter und die dazugehörigen Hashwerte enthalten. Wenn sie an eine Datenbank mit gehashten Kennwörtern gelangen, können sie ein Kennwort in der Hashtabelle nachschlagen. Hashtabellen für Kennwörter, die mehr als einige wenige Zeichen lang sind, belegen allerdings Unmengen von Speicherplatz, deshalb werden sie in Rainbow Tables umgewandelt, um Speicherplatz zu sparen (wobei etwas geringere Geschwindigkeit und Genauigkeit in Kauf genommen werden). Rainbow Tables verwenden komplizierte Mathematik, um Tabellen mit gehashten Einträgen drastisch zu verkleinern. Dabei handelt es sich nicht um Text-, sondern um Binärdateien. Rainbow Tables gehören eigentlich zum Themenkreis von CompTIA Security+- oder noch anspruchsvolleren Zertifizierungen, aber der Begriff ist so gebräuchlich geworden, dass CompTIA A+-Techniker wissen müssen, was er bedeutet.

Wichtig

Für die Prüfung sollten Sie sich merken, das Rainbow Tables dazu verwendet werden, aus Hashwerten auf Kennwörter zu schließen. In der Praxis stellen Rainbow Tables nur für ältere Systeme eine echte Bedrohung dar. Heutige Authentifizierungssysteme fügen den Kennwörtern vor der Berechnung des Hashs zusätzliche Werte hinzu. Dieser Vorgang wird als *Salting* bezeichnet. Wenn die Hashwerte auf diese Weise berechnet werden, sind Rainbow Tables nutzlos.

Pop-ups und Drive-by-Downloads *Pop-ups* sind diese beim Besuch von Webseiten automatisch auftauchenden Browserfenster, die fast immer nur nerven und unerwünscht sind. Es ist nicht ganz einfach, Pop-ups loszuwerden. Ihnen ist sicher schon aufgefallen, dass die meisten Pop-up-Browserfenster gar nicht wie echte Browserfenster aussehen. Es gibt keine Menüleiste, keine Symbolleiste und kein Adressfeld, und doch handelt es sich um separate Browserfenster. Durch HTML-Code können Entwickler von Websites und Werbung die üblichen Navigationshilfen aus Browserfenstern entfernen, sodass Sie nur noch den Inhalt sehen. Wie ich in Kürze erläutern werde, ähneln einige Pop-up-Browserfenster sogar absichtlich Pop-up-Warnungen des Betriebssystems. Oft gibt es auch Schaltflächen, die zwar wie die SCHLIESSEN-Schaltflächen von Windows aussehen, nach dem Anklicken aber nur dafür sorgen, dass noch mehr Pop-ups angezeigt werden! Also, was tun?

Beim Umgang mit Pop-ups müssen Sie zunächst einmal wissen, wie man sie schließt, ohne sie anzuklicken. Wie bereits erwähnt, fehlen in den meisten Pop-ups die Navigationshilfen und sie erscheinen auf dem Bildschirm an einer Position, bei der die SCHLIESSEN-Schaltfläche des Browserfensters (das kleine X oben rechts) außerhalb des sichtbaren Bildschirmbereichs liegt. Einige werden auch hinter dem

aktiven Browserfenster angezeigt und warten dort. Ärgerlich! Um dies zu verhindern, müssen Sie zum Schließen des Pop-up-Fensters anders vorgehen. Beispielsweise können Sie das Symbol für das Browserfenster in der Taskleiste mit der rechten Maustaste anklicken, um sich das Kontextmenü anzeigen zu lassen. Wenn Sie SCHLIESSEN wählen, sollte das Fenster verschwinden. Sie können das fragliche Browserfenster auch über die Tastenkombination [Alt] + [⇆] in den Vordergrund holen und es dann per [Alt] + [F4] schließen.

Die meisten Webbrowser unterstützen Funktionen zur Unterdrückung von Pop-ups, bieten aber leider oft keine Hilfe bei anderen Ärgernissen, mit denen Webnutzer sich heutzutage konfrontiert sehen. Mit Erweiterungen wie beispielsweise uBlock Origin oder Ghostery können Sie eine Vielzahl dieser Plagen steuern, unter anderem Pop-up-Fenster, Cookies und Ad-Tracking. Derartige Erweiterungen lassen sich besser konfigurieren, da Sie hier angeben können, was bei bestimmten Internetadressen erlaubt sein soll. Für Anfänger ist die Vielzahl der Einstellungen aber eher verwirrend.

Eine weitere gebräuchliche Spyware-Methode ist, in Pop-up-Browserfenstern eine scheinbar von Windows stammende Systemwarnung anzuzeigen (Abbildung 27.19). Sobald Sie diese anklicken, wird eine Flut weiterer Browserfenster angezeigt oder womöglich sogar eine Datei heruntergeladen. Das ungewollte, unwissentliche oder nicht beabsichtigte Herunterladen von Dateien wird auch als *Drive-by-Download* bezeichnet.

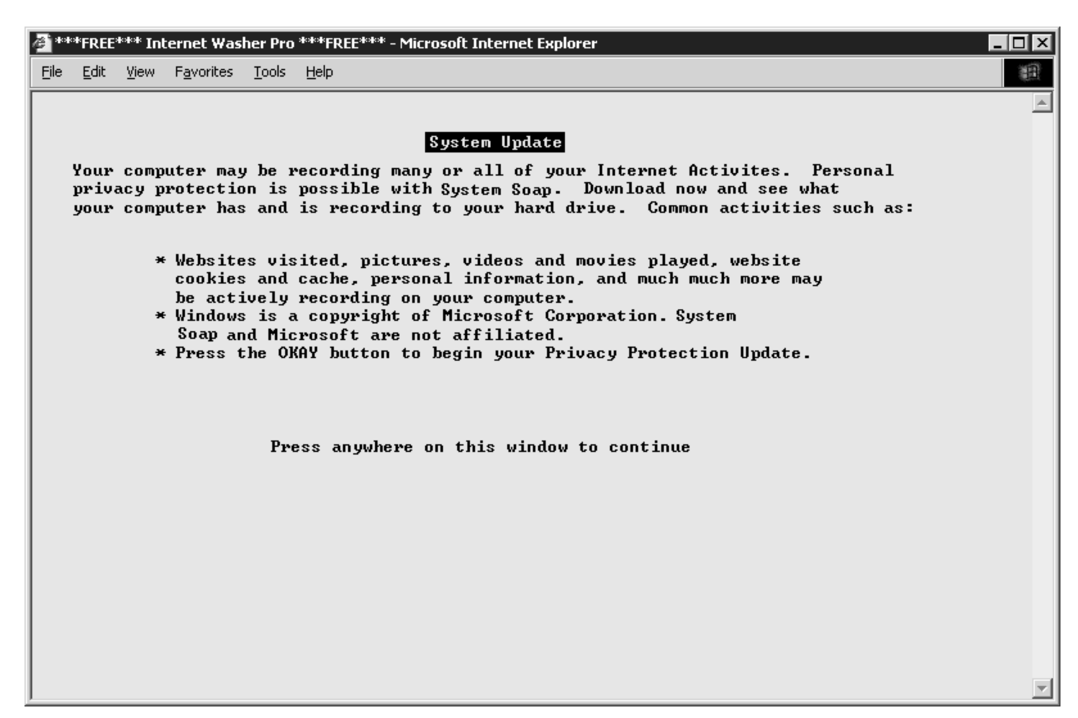


Abb. 27.19: Ein Pop-up-Browserfenster von einer Spyware, wie sich als Windows-Warnung tarnt

Die Lektion ist einfach – *installieren Sie diese Programme nicht!* Jedenfalls nicht, ohne vorher Nachforschungen über das verdächtige Programm anzustellen. Wenn Sie eine Website besuchen und aufgefordert werden, ein Programm von einem Drittanbieter oder ein Plug-in zu installieren, von dem Sie nie zuvor gehört haben, dann *installieren Sie es nicht!* Bekannte und vertrauenswürdige Plug-ins, wie beispielsweise Flash von Adobe, sind ungefährlich, aber allen anderen gegenüber sollten Sie misstrauisch sein. Klicken Sie nicht einfach irgendwo in ein Pop-up-Browserfenster, auch wenn es wie eine Warnung von Windows oder wie eine DOS-Eingabeaufforderung aussieht, denn wie eben erwähnt, ist es sehr wahrscheinlich gefälscht, und bei der SCHLIESSEN-Schaltfläche handelt es sich eigentlich um

einen Hyperlink. Schließen Sie das Fenster auf andere Weise, wie beispielsweise mit `Alt` + `F4` oder indem Sie das Browserfenster-Symbol in der Taskleiste mit der rechten Maustaste anklicken und SCHLIESSEN wählen.

Sie können auch Software zur Erkennung und Entfernung von Spyware auf Ihrem System installieren und regelmäßig ausführen. Das werden wir uns nun einmal etwas genauer ansehen.

Einige Spyware-Hersteller sind immerhin so anständig, dass sie Routinen zur Deinstallation ihrer Software bereitstellen. Gator-Programme werden Sie beispielsweise ganz einfach los, indem Sie diese über das Applet SOFTWARE bzw. PROGRAMME UND FEATURES in der Systemsteuerung entfernen. Andere dagegen sind nicht so kooperativ. Weil Spyware so hinterhältig ist, kann es sein, dass auf Ihrem System bereits entsprechende Programme installiert sind, ohne dass Sie es wissen.

Windows beinhaltet den *Windows Defender* (Abbildung 27.20), der in Windows 10 einfach nur VIREN- & BEDROHUNGSSCHUTZ heißt, ein praktisches Werkzeug zum Erkennen von Spyware, das aber auch nicht perfekt ist. Die bessere Lösung ist es, den Windows Defender mit einem zweiten Programm zum Entfernen von Spyware zu ergänzen. Mein persönlicher Favorit ist Malwarebytes.



Abb. 27.20: Viren- & Bedrohungsschutz

Das Programm funktioniert wie versprochen. Es erkennt und löscht Spyware aller Art – verborgene Dateien und Ordner, Cookies, Registry-Schlüssel (Registry keys) und -werte usw. Malwarebytes ist für den privaten Gebrauch kostenlos. Abbildung 27.21 zeigt Malwarebytes in Aktion.

Tipp

Falls Sie es noch nicht getan haben: Besuchen Sie `http://www.malwarebytes.com` und laden Sie sich die neueste Version herunter. Installieren Sie das Programm und führen Sie es aus. Findet es irgendwelche Schadsoftware, die Ihnen entgangen ist?

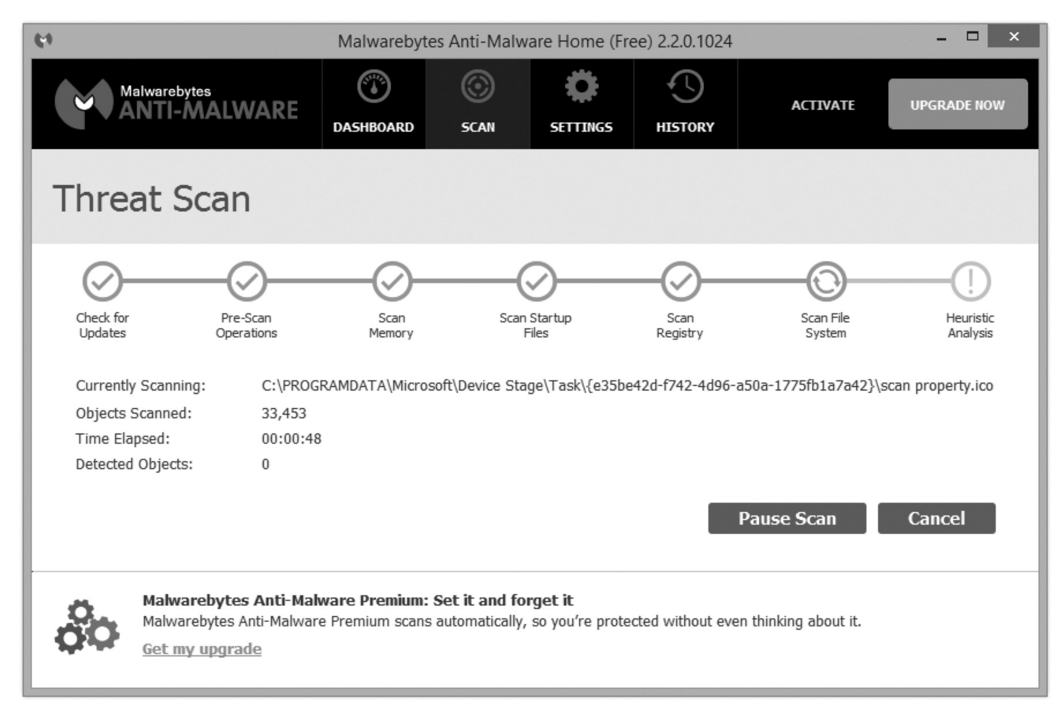


Abb. 27.21: Malwarebytes

Spam E-Mails, bei deren Absender es sich nicht um Freunde, Familienmitglieder oder Kollegen handelt und die Sie nicht angefordert haben, können für Ihren Rechner und Sie selbst riesiges Gefahrenpotenzial bergen. Diese unerwünschten E-Mails, die auch als *Spam* bezeichnet werden, sind für einen Großteil des Datenverkehrs im Internet verantwortlich. Spam gibt es in unterschiedlichen Varianten von Unternehmen, die Ihnen nur ihre Produkte verkaufen wollen, bis hin zu Betrügern, die einfach nur Ihr Geld wollen. Hoaxes, Pornografie und Schneeballsysteme füllen den Posteingang vieler E-Mail-Benutzer. Viel Zeitverschwendung, die einem leicht auf die Nerven gehen kann.

Es gibt mehrere Möglichkeiten zur Bewältigung der Spam-Flut. Zunächst einmal können Sie sich schützen, indem Sie Ihre E-Mail-Adresse nicht im Internet veröffentlichen, sofern Sie dazu nicht aus juristischen Gründen gezwungen sind. Spammer durchsuchen das Internet nach veröffentlichten Adressen.

Filter und Filtersoftware können Spam auf Ihrem Mailserver und Computer blockieren. Gmail verfügt beispielsweise über leistungsfähige Filter, mit denen die Zahl der durchschnittlich von den Abonnenten empfangenen Spam-E-Mails wesentlich reduziert werden konnte, oft um mehr als 90 Prozent. Sie können die meisten E-Mail-Programme so einstellen, dass sie E-Mail bestimmter Absender (praktisch, wenn Ihnen jemand auf die Nerven geht) oder bestimmter Empfänger blockieren. Sie können E-Mails mit bestimmten Inhalten der Betreffzeile oder anhand von Schlüsselwörtern filtern.

Viele Spam-E-Mails enthalten im Anhang Schadsoftware oder verweisen auf gefährliche Websites. Klicken Sie niemals auf die Links in Spam-E-Mails oder öffnen Sie diese E-Mails besser gar nicht, wenn Ihnen der Absender unbekannt ist, denn damit schützen Sie möglicherweise Ihren Computer vor Schadsoftware.

Spam ist außerdem für Betrügereien durch *Phishing* berüchtigt. Dabei erhalten Sie eine E-Mail, die auf den ersten Blick seriös erscheint, wie z.B. eine Rechnung, eine Auftragsbestätigung oder Konteninformationen, durch die Sie dazu gebracht werden sollen, Zugangsdaten oder persönliche Daten preiszugeben. Wenn Sie derartige E-Mails erhalten, die angeblich von Amazon, eBay oder Ihrer Bank

stammen, ignorieren Sie diese besser. Platzieren Sie den Mauszeiger über dem Link, um die tatsächliche Adresse anzuzeigen, die wahrscheinlich nicht das ist, was sie zu sein vorgibt. Holzauge, sei wachsam!

27.3.2 Anzeichen und Symptome für Schadsoftware

Falls Ihr PC mit einer Schadsoftware infiziert ist, werden Sie über einige eigentümliche Dinge stolpern, die Sie überhaupt erst auf den Gedanken bringen, nach Schadsoftware zu suchen. Schadsoftware verursacht, ähnlich einer Erkrankung, ungewöhnliche Symptome, die bei der üblichen Computernutzung nicht auftreten. Um diese verschiedenen Symptome richtig zu deuten, müssen Sie zum PC-Doktor werden!

Schadsoftware ist ungemein flexibel und kann in jeder erdenklichen Form erscheinen. Tatsächlich wirken manche Malware-Angriffe wie der gewöhnliche »Schluckauf«, der bei der täglichen Arbeit schon mal aufkommt: kurze Aussetzer bei der Arbeitsgeschwindigkeit, zufällige, einmalige Systemabstürze usw. Wenn Sie erkennen, dass sich ein merkwürdiger Programmabsturz auf eine Schadsoftware zurückzuführen lässt, ist das schon die halbe Miete.

Wenn der PC langsam arbeitet, kann das ein Zeichen dafür sein, dass Sie zu viele Programme gleichzeitig ausführen, möglicherweise aber auch, dass der Computer von Malware befallen ist. Wie lässt sich das unterscheiden? Im vorliegenden Fall durch die Häufigkeit, mit der das Problem auftritt. Geschieht dies öfter, selbst wenn alle Anwendungen beendet sind, haben Sie den Ärger am Hals. Das gilt auch bei mehrfachem, kurzem Einfrieren. Falls sich Windows nicht ordentlich benimmt (mehr als sonst), starten Sie besser gleich Ihre Anti-Malware-Software.

Es muss aber nicht notwendigerweise zu Systemabstürzen kommen, wenn eine Schadsoftware aktiv ist. Mache Malware versucht, Systemdateien umzubenennen, Zugriffsrechte zu ändern oder Dateien zu verbergen. Möglicherweise erhalten Sie auch E-Mails von Kollegen oder Bekannten, die sich danach erkundigen, was es denn mit der Nachricht von »Ihnen« auf sich habe, die doch sehr nach Spam aussah. Vielleicht bekommen Sie auch Abwesenheitsnotizen von E-Mail-Adressen, an die Sie ganz bestimmt keine Nachricht versendet haben. Diese Art von Schadsoftware wird gewöhnlich beim regelmäßigen Scannen nach Malware gefunden. Solange Sie wachsam bleiben, haben Sie also nichts zu befürchten.

Wichtig

Es muss sich nicht gleich um einen Malware-Angriff handeln, aber achten Sie auch auf eigene E-Mail-Konten oder Konten von Bekannten, die plötzlich vermehrt befremdliche Nachrichten empfangen. Die Hacker greifen sowohl Webmail- als auch E-Mail-Client-Benutzer an. Ändern Sie in diesem Fall Benutzername und Kennwort beim Webmailer bzw. führen Sie auf dem Rechner einen Malware-Scan durch.

Manche Malware versucht auch, sich gegen Ihre vielfältigen Versuche, sie zu entfernen, zu wehren. Wenn Windows Update unversehens nicht mehr funktioniert und Sie Ihr System daher nicht mehr patchen können, ist der PC vermutlich mit Malware infiziert. Wenn andere Werkzeuge und Dienstprogramme Ihnen unvermittelt Knüppel in Form von »Zugriff verweigert«-Meldungen zwischen die Beine werfen, ist das ebenfalls ein Hinweis auf Schadsoftware. Sollte Ihre Internetverbindung nicht mehr funktionieren, steckt entweder die Malware dahinter oder aber die Verbindung wurde durch das Entfernen der Malware unterbrochen. Unter Umständen ist es dann erforderlich, Ihre Internetverbindung erneut einzurichten: Neuinstallation von Netzwerkkarte und deren Treiber, Neustart des Routers usw.

Selbst Ihr Webbrowser und Ihre Anti-Malware-Software können sich gegen Sie wenden. Wenn Sie nach der Eingabe einer Internetadresse auf einer anderen Website landen als erwartet, hat vielleicht eine Schadsoftware Ihre `HOSTS`-Datei überschrieben. Die `HOSTS`-Datei hat Vorrang vor den DNS-Einstellungen und kann Ihren Webbrowser auf jede beliebige Website umleiten, die eine Schadsoftware dort einträgt. Meistens werden Sie auf Phishing-Websites oder auf Websites mit kostenlosen Program-

men (die natürlich mit Malware gespickt sind) umgeleitet. Tatsächlich handelt es sich bei manchen kostenlosen *Anti*-Malware-Programmen in Wahrheit um Malware – Techniker nennen das manchmal *Schurken-Anti-Malware*. Halten Sie sich lieber an die Listen empfohlener Anti-Malware-Software, die Sie auf renommierten Websites wie Ars Technica, Tom's Hardware oder Anandtech finden können.

Wichtig

In den Lernzielen der Prüfung 1002 wird `system/application log errors` als Symptom genannt. Manche Schadsoftware hinterlässt in diesen Protokolldateien tatsächlich Spuren, die Hinweise darauf enthalten können, was die Schadsoftware unternehmen wollte. Möglicherweise entdecken Sie, dass versucht wurde, Dienste zu deaktivieren, die Ihr System schützen oder Warnungen bei hoher Auslastung von Ressourcen anzeigen. Wenn hier Muster erkennbar sind, kann das ein Hinweis auf Schadsoftware sein. Allerdings werden Sie oder Ihre Benutzer fast mit Sicherheit andere Symptome bemerken, bevor es erforderlich wäre, in diesen Dateien nach Unregelmäßigkeiten zu suchen.

Beachten Sie die Sicherheitswarnmeldungen, die möglicherweise von Windows selbst oder von Ihrem Anti-Malware-Programm eines Drittanbieters angezeigt werden. Die in Windows integrierten Werkzeuge benachrichtigen Sie über das WARTUNGSCENTER, das Sie in Kapitel 16 schon kennengelernt haben (Abbildung 27.22), oder in Windows 10 über die Einstellung WINDOWS-SICHERHEIT. Viel zu konfigurieren gibt es in diesen Applets eigentlich nicht, sie zeigen aber an, ob der Rechner geschützt ist oder nicht. Beide Applets platzieren im Infobereich der Taskleiste ein Symbol und blenden eine Benachrichtigung ein, sobald ein Problem entdeckt wird.

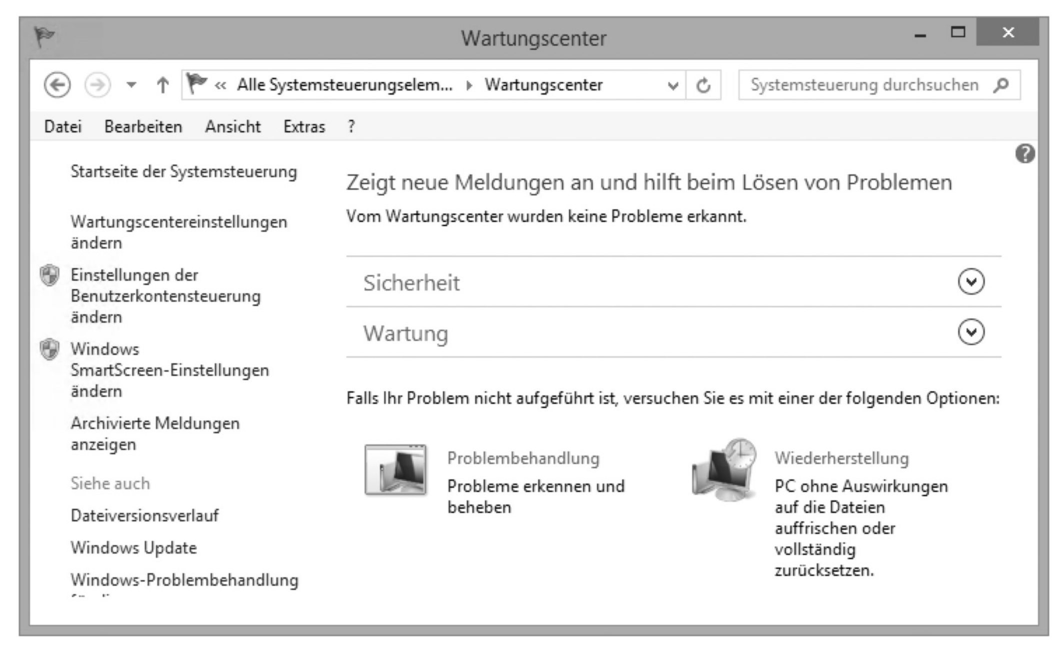


Abb. 27.22: Das Wartungscenter in Windows 8.1

27.3.3 Schadsoftware: Vorbeugen und Wiederherstellen

Sie können Ihren PC nur dann dauerhaft vor Malware schützen, wenn Sie ihn vom Internet trennen und auf keinen Fall weitere, potenziell infizierte Software installieren. Da diese beiden Vorgehensweisen heutzutage unrealistisch sind, kommt stattdessen spezielle Anti-Malware-Software zum Einsatz,

um die unausweichlichen Angriffe abzuwehren. Aber auch die besten Anti-Malware-Programme vermögen es nicht immer zu verhindern, dass sich Schadsoftware auf Ihrem Computer einschleicht. Wenn Sie feststellen, dass Systeme infiziert sind, müssen Sie der weiteren Verbreitung der Malware Einhalt gebieten und sie von infizierten Rechnern entfernen, um den ursprünglichen Zustand so gut wie möglich wiederherzustellen.

Schadsoftware bewältigen

Es gibt verschiedene Möglichkeiten, mit Malware fertig zu werden. Sie können Anti-Malware-Software (Antivirenprogramme) verwenden, Schulungen durchführen, um bei den Anwendern das Bewusstsein für Schadsoftware zu schärfen, eine Strategie für die Softwareaktualisierung umsetzen oder eine einfache Möglichkeit zur Wiederherstellung der Systeme schaffen, wenn es zu Problemen kommt.

Dass auf allen Computern zumindest ein Antivirenprogramm läuft, ist eigentlich selbstverständlich. Falls die Möglichkeit besteht, sollten Sie eine Hardware-Firewall einsetzen, die alle von extern eingehenden Daten auf Schadsoftware überprüft, bevor diese in Ihr Netzwerk gelangen. Sie müssen auch berücksichtigen, dass jede Schutzsoftware auf buchstäblich tägliche Aktualisierungen angewiesen ist, um die neuesten Bedrohungen zu erkennen. Den Anwendern muss auch klar sein, dass sie nicht bei jeder fragwürdigen Werbung, suspekten Programmen oder Pop-ups wahllos Links anklicken dürfen. Gut über Malware unterrichtete Benutzer erkennen mögliche Gefahren. Für den Fall, dass sich tatsächlich Schadsoftware bei Ihnen einnistet, sollte es Richtlinien und Handlungsanweisungen geben, damit alle Anwender wissen, was dann zu tun ist. Nicht zuletzt führt jeder gute Techniker Buch über derartige Zwischenfälle, um gegebenenfalls Regelmäßigkeiten bei den Angriffen zu erkennen. Die Sicherheitsrichtlinien können dann dementsprechend angepasst werden.

Wichtig

Die konsequente Aktualisierung der Software der von Ihnen betreuten Systeme gehört zu den wichtigsten Maßnahmen zum Schutz vor Malware. Microsoft, Apple und die Linux-Distributionen leisten bei der Bereitstellung von Fehlerbehebungen und Patches im Allgemeinen sehr ordentliche Arbeit, sobald Probleme bekannt werden. Falls Sie automatische Updates deaktiviert haben, sollten Sie wenigstens regelmäßig nach Aktualisierungen suchen und diese installieren.

Anti-Malware-Programme

Schutzsoftware wie die klassischen *Antivirenprogramme* schützen Rechner auf aktive und passive Weise. Sie können sowohl aktiv Viren aufspüren und entfernen als auch passiv als Wachposten dienen. Wenn das Programm Viren suchen und entfernen soll, durchsucht es den Bootsektor des Computers und danach alle Dateien. Wenn es Viren erkennt, zeigt es die verfügbaren Optionen zu deren Entfernung oder Deaktivierung an. Antivirenprogramme können auch als *Virenschild* dienen, die Aktivitäten Ihres Computers passiv überwachen und nur bei bestimmten Ereignissen nach Viren suchen, wie z.B. bei der Ausführung von Programmen oder dem Herunterladen von Dateien.

Hinweis

Der Begriff »Antivirus« (oder Anti-Spyware oder Anti-Sonstwas) veraltet allmählich. Viren machen nur einen geringen Teil der vielen verschiedenen Arten von Malware aus. Für viele Leute ist der Ausdruck aber weiterhin gleichbedeutend mit Anti-Malware.

Antivirenprogramme verwenden unterschiedliche Techniken zur Bekämpfung der verschiedenen Virentypen. Sie erkennen Bootsektorviren durch Vergleichen des Bootsektors eines Laufwerks mit einem Standardbootsektor. Das funktioniert, weil die meisten Bootsektoren grundsätzlich identisch sind. Einige Antivirenprogramme legen Sicherungskopien des Bootsektors an. Wenn sie ein Virus erkennen, ersetzen sie den infizierten Bootsektor wieder durch die Sicherungskopie. Ausführbare

Viren sind etwas schwieriger zu erkennen, weil sie sich in allen ausführbaren Dateien befinden können. Um sie erkennen zu können, verwenden Antivirenprogramme Signaturbibliotheken. Bei *Signaturen* handelt es sich um typische Codemuster bekannter Viren. Das Antivirenprogramm vergleicht die ausführbaren Dateien mit seiner Signaturbibliothek. Es gibt aber durchaus auch Fälle, in denen völlig saubere Programme zufällig Code enthalten, der dem in den Signaturbibliotheken gespeicherten Codemustern von Viren entspricht. Normalerweise sorgen die Hersteller der Antivirenprogramme dann schnell für einen Patch, um weitere Fehlalarme zu vermeiden.

Wichtig

Rechnen Sie in der CompTIA A+-Zertifizierungsprüfung 1002 mit Fragen zum Thema dubiose Antivirensoftware. Damit kann zweierlei gemeint sein: Zum einen ein Trojaner, also ein Programm, das scheinbar nützlich ist, tatsächlich aber Ihren Rechner infiziert. Oder zum anderen miserabel programmierte Anti-Malware, die Ihren Computer zwar schützt, aber zu dem Preis, dass er nicht mehr ordentlich läuft. In der Prüfung kommt vermutlich eher die erste Bedeutung vor.

Da Sie nun wissen, welche Virentypen es gibt und wie Antivirenprogramme versuchen, davor zu schützen, wollen wir uns mit einigen Begriffen befassen, die bei der Beschreibung bestimmter Virengefahren immer wieder verwendet werden.

Tipp

Sehen Sie sich unter `http://totalsem.com/100x` unbedingt die Übung zum Thema Viren im Bereich zu Kapitel 27 an!

Polymorphe Viren *Polymorphe Viren* versuchen, ihre Signatur zu ändern, um die Erkennung durch Antivirenprogramme zu verhindern. Dazu verändern sie normalerweise kleine Abschnitte nutzlosen Codes. Glücklicherweise kann der veränderte Code identifiziert und als Signatur verwendet werden – nachdem die Antivirenhersteller auf das Virus aufmerksam geworden sind. Eine Technik, sich gegen unbekannte polymorphe Viren zu schützen, ist der Einsatz von Antivirenprogrammen, die Prüfsummen für alle Dateien auf dem Laufwerk anlegen. Bei der Prüfsumme handelt es sich hier um eine Zahl, die vom Programm in Abhängigkeit vom Dateiinhalt (nicht von Name, Datum oder Größe) berechnet wird. Die Algorithmen für die Erstellung dieser Prüfsummen unterscheiden sich bei den einzelnen Antivirenprogrammen (sie werden normalerweise auch geheim gehalten, um Virenentwicklern keine Möglichkeit für Gegenmaßnahmen zu bieten). Immer wenn ein Programm ausgeführt wird, berechnet das Antivirenprogramm die Prüfsumme neu und vergleicht sie mit seinen früheren Berechnungen. Wenn sich die Prüfsummen unterscheiden, ist das ein sicherer Hinweis auf ein Virus.

Stealth-Viren Bei den »getarnten« Viren (Stealth-Viren) handelt es sich mehr um ein Konzept als um eine echte Virenfunktion. Die meisten getarnten Virenprogramme sind Bootsektorviren, die verschiedene Methoden anwenden, um sich vor der Antivirensoftware zu verbergen. Das Stealth-Virus AntiEXE beispielsweise hängt sich an einen wenig bekannten, aber häufig verwendeten Software-Interrupt an und läuft nur dann, wenn dieser ausgeführt wird. Andere legen Kopien unverdächtig aussehender Dateien an.

Anwenderschulung

Zur Vermeidung von Malware-Angriffen und zur Verminderung von Folgeschäden sollten Sie die Benutzer gut darauf vorbereiten. Vermitteln Sie den Benutzern, bei eingehenden E-Mails von unbekannten Absendern Vorsicht walten zu lassen und keine Anhänge oder URLs zu öffnen, wenn sie sich der Herkunft der E-Mail nicht hundertprozentig sicher sind.

Erläutern Sie die Gefahren fragwürdiger Websites und zeigen Sie den Anwendern, wie sie beim Erscheinen solcher Websites vorgehen sollten. Alle Webbrowser zeigen beim Aufsuchen bekanntermaßen bösartiger Websites Warnhinweise wie in Abbildung 27.23 an.

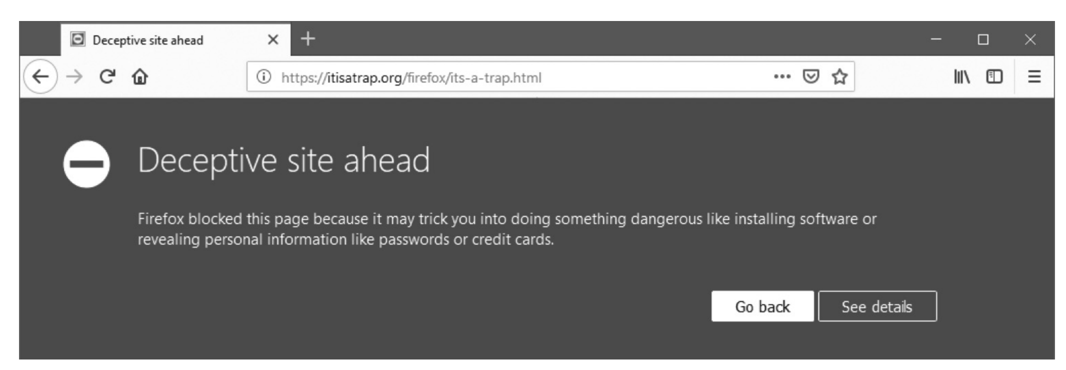


Abb. 27.23: Warnung vor einer bösartigen Website

Niemand möchte von Malware infiziert werden. Die Anwender sind motiviert und erfreut, wenn Sie ihnen dabei helfen, sich selbst zu schützen. Und letzten Endes machen gut informierte, sicherheitsbewusste Anwender Ihnen das Leben ebenfalls leichter.

Tipps zur Vorbeugung

Am besten vermeidet man Schäden durch bösartige Softwareangriffe dadurch, dass man sich die Malware gar nicht erst einfängt. Eine Möglichkeit ist die Verwendung einer Variante des klassischen DNS, nämlich *SecureDNS*. Der DNS-Anbieter implementiert zusätzliche Filter, um zu verhindern, dass Ihr System alle möglichen bösartigen Websites aufsucht. Wenn Sie nicht verhindern können, dass Ihr System für Schadsoftware erreichbar ist, sollte sie zumindest abgefangen werden, wenn sie sich auf Ihrem Computer einnisten will. Wie bereits erwähnt, beinhalten alle guten Antivirenprogramme einen Virenschild, der E-Mails, Downloads, ausgeführte Programme usw. automatisch überprüft (Abbildung 27.24).



Abb. 27.24: Aktivierter Antivirenschild in Windows 10

Nutzen Sie Ihren Antivirenschild. Sie sollten PCs permanent gegen mögliche Virenangriffe schützen. Alle Antivirenlösungen beinhalten Programme, die nach dem Rechnerstart im Hintergrund ausgeführt werden (TSR-Programme – *Terminate-and-Stay Resident*). Außerdem sollten Sie sich über die Herkunft von Software informieren, bevor Sie diese herunterladen. Installieren Sie nur Software, die vertrauenswürdigen Quellen entstammt, wie z.B. der Website des Herstellers oder einem App-Store wie Valves Steam-Dienst. Vermeiden Sie Software aus nicht vertrauenswürdigen Quellen um jeden Preis, beispielsweise die kostenlosen Programme zum Bereinigen der Registry, die auf irgendwelchen `.support`-Domänen zu finden sind.

Halten Sie Ihre Antiviren- und Anti-Malware-Software stets auf dem neuesten Stand. Neue Schadsoftware und Viren erscheinen täglich, und Ihr Programm sollte diese kennen. Die Liste der Viren, die Ihr Antivirenprogramm erkennen kann, wird in *Definitionsdateien* verwaltet, die Sie aktuell halten sollten. Glücklicherweise aktualisieren sich die meisten Antivirenprogramme automatisch. Darüber hinaus sollten Sie das Kernprogramm (die sogenannte *Engine*) mit der »Virensuchmaschine« von Zeit zu Zeit aktualisieren, um auch in den Genuss der aktuellen Verbesserungen zu kommen.

Tipp: Empfehlenswerte Anti-Malware-Software

Es gibt eine Reihe hervorragender kostenlos herunterladbarer Anti-Malware-Programme (mit langer Testphase oder unbeschränkter Nutzungsdauer). Da Sie um den Einsatz von Anti-Malware nicht herumkommen, wenn Sie Ihre Systeme schützen möchten, sollten Sie sich eins oder mehrere der folgenden Programme herunterladen:

- **Malwarebytes** (`www.malwarebytes.org`): Malwarebytes ist kaum zu schlagen, wenn es darum geht, mit bösartiger Software fertig zu werden. Es gibt sowohl eine kostenlose Version, mit der Sie nach Malware scannen und diese unter Quarantäne stellen können, als auch eine Premium-Version, die aktiv vor der Infizierung mit Malware schützt. Dieses Programm ist meine erste Wahl, wenn ich auf dem Computer eines Kunden Malware vorfinde.
- **Adaware** (`http://www.adaware.com`): Adaware ist ein ausgezeichnetes Anti-Malware-Programm. Adaware Antivirus bietet kostenlosen Schutz vor Viren und Spyware und stöbert alle möglichen Dateien und Programme auf, die Ihren Computer unnötig verlangsamen (oder noch Schlimmeres anrichten) und entfernt sie. Das kostenpflichtige Adaware Antivirus Pro bietet erweiterten Schutz durch eine Zwei-Wege-Firewall, Bedrohungsblockieralgorithmen und Schutz vor Phishing.
- **Spybot** (`www.safer-networking.com`): Spybot von Safer Networking Ltd. ist ein weiteres erstklassiges Anti-Malware-/Anti-Spyware-Programm. Viele Leute setzen sowohl Adaware als auch Spybot ein und es kommt vor, dass sich die beiden Programme gegenseitig als Spyware klassifizieren! Es sind außerdem Home- und Pro-Versionen verfügbar, die zusätzlichen Schutz und weitere Features bieten.

Startfähige Medien zur Malware-Bekämpfung

Wenn sich Ihr Computer trotz Verwendung einer Anti-Malware-Software dennoch mit Schadsoftware infiziert (insbesondere nach einem Neustart), müssen Sie zu härteren Mitteln greifen. Viele Hersteller von Anti-Malware-Software bieten startfähige CDs oder USB-Speichersticks an (oder liefern Anleitungen, wie Sie diese selbst erstellen können). Auf diese Weise können Sie von einem mit Sicherheit sauberen System starten und die Anti-Malware ausführen, ohne dabei durch die vorhandene Malware behindert zu werden.

Tipps zur Beseitigung von Malware

Wenn das Unvermeidbare geschieht und Ihr eigener Rechner oder der eines Anwenders von Malware wie etwa einem Computervirus befallen wird, dann müssen Sie verhindern, dass sich das Problem weiter ausbreitet und dafür sorgen, dass der befallene Computer möglichst schnell wieder einsatzbereit ist. Die CompTIA sieht folgende Schritte vor:

1. Erkennung der Malware-Symptome
2. Infiziertes System unter Quarantäne stellen

3. Systemwiederherstellung deaktivieren (in Windows)
4. Wiederherstellung des infizierten Systems
   a) Aktualisierung der Anti-Malware-Software
   b) Suchen und entfernen (Abgesicherter Modus, Vorinstallationsumgebung)
5. Überprüfungen und Aktualisierungen planen
6. Systemwiederherstellung aktivieren und Wiederherstellungspunkt erstellen (in Windows)
7. Anwenderschulung

Wichtig

Neben dieser Vorgehensweise nennen die Lernziele der Prüfung 1002 auch eine vollständige Wiederherstellung anhand eines Backups als eine Möglichkeit, zu gewährleisten, dass ein System frei von Schadsoftware ist. Dabei gibt es jedoch unter Umständen Schwierigkeiten.

Sie benötigen natürlich Speicherplatz, um vollständige Backups des Systems zu erstellen, und müssen weit genug vorausplanen, damit ein möglichst aktuelles Backup verfügbar ist. Zudem müssen Sie sich sicher sein, dass mindestens eins der Backups nicht von der Schadsoftware infiziert ist. Darüber hinaus müssen Sie entweder die Benutzerdaten separat sichern oder aber in Kauf nehmen, dass die seit dem letzten Backup neu erstellten oder geänderten Dateien verloren gehen. Es wäre sinnvoll, die Benutzerdaten *separat* zu sichern und ein vollständiges Backup des Systems selbst zu erstellen, nachdem die benötigte Software installiert und konfiguriert ist, aber diese Option ist nicht immer verfügbar.

Erkennung und Quarantäne Im ersten Schritt müssen Sie erkennen, dass ein potenzieller Malware-Befall stattgefunden hat. Wenn Sie beispielsweise den Datenverkehr im Netzwerk überwachen und feststellen, dass ein Computer plötzlich massenhaft E-Mails versendet, ist das schon ein deutlicher Hinweis. Oder Anwender beschweren sich vielleicht darüber, dass ein gestern noch flotter Rechner heute plötzlich zu einer lahmen Schnecke geworden ist.

In vielen Netzwerken wird Software eingesetzt, wie z.B. das quelloffene Programm *PacketFence*, die den Netzverkehr überwacht und Rechner automatisch vom Netz nehmen kann, wenn diese plötzlich verdächtige Datenpakete versenden. Sie können einen Computer natürlich auch von Hand unter Quarantäne stellen, indem Sie das Netzwerkkabel abziehen. Sobald Sie dafür gesorgt haben, dass der Rechner keine anderen anstecken kann, können Sie das Virus oder andere Malware suchen und beseitigen.

Sie sollten an dieser Stelle außerdem die Systemwiedereherstellung deaktivieren. Wenn Sie irgendwelche Fortschritte erzielen, möchten Sie natürlich nicht, dass die Malware in Wiederherstellungspunkten enthalten ist. Öffnen Sie in Windows in der Systemsteuerung das Applet SYSTEM und klicken Sie in der Aufgabenliste links auf COMPUTERSCHUTZ. Wählen Sie auf der gleichnamigen Registerkarte ein Laufwerk aus und klicken Sie auf KONFIGURIEREN. Wählen Sie dann im Dialogfeld SYSTEMSCHUTZ, das nun geöffnet wird, COMPUTERSCHUTZ DEAKTIVIEREN aus. Wiederholen Sie diesen Vorgang mit allen Laufwerken des Systems.

Suchen und entfernen Wenn Sie den oder die befallenen Rechner isoliert haben, müssen Sie für eine sichere Startumgebung sorgen und Anti-Malware-Software ausführen. Zunächst können Sie in Windows 7 den abgesicherten Modus bzw. in Windows 8/8.1/10 die Wiederherstellungsumgebung ausprobieren, da Sie dafür nur den Rechner neu starten müssen. Wenn das nicht funktioniert oder wenn Sie ein Bootsektor-Virus vermuten, dann müssen Sie externe startfähige Medien verwenden, wie z.B. ein bootfähiges optisches Medium oder einen USB-Speicherstick.

Gewöhnen Sie sich an, einen startfähigen USB-Speicherstick oder ein bootfähiges optisches Medium mit der Anti-Malware-Software bereitzuhalten. Wenn Sie ein Virus oder andere Malware vermuten, sollten Sie zum Starten das externe Medium verwenden, selbst wenn Ihre Anti-Malware-Software behauptet, das Problem beseitigt zu haben. Schalten Sie den PC aus und starten Sie ihn vom externen Medium neu. (Möglicherweise müssen Sie die CMOS-Einstellungen ändern, um von dem externen

Medium booten zu können.) Damit erhalten Sie eine saubere Startumgebung, von der Sie wissen, dass sie frei von irgendwelchen Bootsektor-Viren ist. Falls Sie nur relativ aktuelle Systeme betreuen, werden Sie vermutlich einen USB-Speicherstick bevorzugen, um schneller starten zu können.

Es gibt mehrere Möglichkeiten, um eine startfähige CD/DVD oder einen bootfähigen USB-Speicherstick zu erstellen. Zunächst einmal gibt es von einigen Antivirenprogrammen bootfähige Versionen. Dann können Sie Linux-Versionen herunterladen, von denen es LiveCDs oder LiveDVDs gibt, wie z.B. *Ubuntu*. Mit einer LiveDVD können Sie den Rechner starten und eine vollständig funktionsfähige Version des Betriebssystems in den Arbeitsspeicher laden, ohne dabei die Daten auf der Festplatte zu ändern oder auch nur darauf zuzugreifen, um vollen Zugriff auf das Internet und die vielen Antiviren-Websites zu erlangen.

Sie können sich darüber hinaus auch eine Kopie der *Ultimate Boot CD* herunterladen und brennen. Sie umfasst einige Antiviren- und Anti-Malware-Programme, weshalb Sie keine weiteren Dienstprogramme benötigen. Sie finden sie unter `www.ultimatebootcd.com`. Der einzige Nachteil besteht dabei darin, dass die Suchmaschinen der Anti-Malware-Programme und auch deren Definitionsdateien relativ schnell veralten.

Sobald eine Startumgebung verfügbar ist, können Sie Ihre Anti-Malware-Software aktualisieren. Starten Sie dann den gründlichsten Scanvorgang der Software. Überprüfen Sie auch alle Wechseldatenträger, die mit dem infizierten System in Berührung gekommen sind und andere Systeme, die Daten von ihm erhalten haben oder über das Netzwerk damit verbunden waren. Viren oder Schadsoftware können manchmal monatelang vor sich hin schlummern, bevor man ihr Vorhandensein bemerkt.

E-Mail ist nach wie vor häufig die Quelle von Viren – schon das Öffnen eines E-Mail-Anhangs kann zu einer Infizierung führen. Auch die Anzeige in einem Vorschaufenster öffnet womöglich den Anhang und kann einen Rechner infizieren. Laden Sie Dateien nur von bekanntermaßen sicheren Seiten herunter und meiden Sie die weniger seriösen Ecken des Internets, denn dort ist es am wahrscheinlichsten, sich Malware einzufangen.

Wichtig

Die CompTIA betrachtet die Entfernung der Malware als Teil der Wiederherstellung. Da man allerdings die Wiederherstellung erst nach dem Entfernen der Malware durchführen kann, habe ich die einzelnen Schritte in der hier gezeigten Reihenfolge aufgeführt.

Wiederherstellung Malware-Infektionen können bei einem System eine Menge Schäden anrichten und insbesondere wichtige Dateien zerstören, die für den Start von Windows benötigt werden. Daher müssen Sie ein zuvor infiziertes System nach der Bereinigung der Laufwerke möglicherweise reparieren. Bei der *Wiederherstellung* geht es einfach darum, dass Sie die von einem Virus oder anderer Malware verursachten Schäden beheben. Dazu müssen Sie vielleicht beschädigte Dateien der Registry oder sogar Startdateien ersetzen.

Wenn Sie Windows nach einem abgeschlossenen Malware-Scan nicht starten können, dann müssen Sie die Windows-Vorinstallationsumgebung booten und die Optionen der Windows-Wiederherstellungsumgebung bzw. der Systemwiederherstellung verwenden.

In der Wiederherstellungsumgebung (siehe Kapitel 16) stehen Ihnen weitere Reparaturwerkzeuge zur Verfügung, zu denen Systemwiederherstellung, Systemimage-Wiederherstellung, Starthilfe und die Eingabeaufforderung zählen (Abbildung 27.25). Wenn Sie die für die jeweilige Situation geeignete Option starten, sollte der Rechner schnell wieder betriebsbereit sein.

Tipp

Denken Sie daran, die Systemwiederherstellung wieder zu aktivieren und einen Wiederherstellungspunkt anzulegen, nachdem das System repariert worden ist.



Abb. 27.25: Optionen bei der Systemwiederherstellung

Anwenderschulung Am besten kann man sich vor Malware schützen, wenn man gut darüber Bescheid weiß. Als IT-Sachverständiger müssen Sie mit Benutzern – insbesondere mit denjenigen, deren Systeme Sie gerade bereinigt haben – darüber sprechen, wie sie sich besser schützen können. Zeigen Sie ihnen Beispiele für gefährliche E-Mails, die sie nicht öffnen sollten, Websites, die sie meiden sollten, und die Art von Programmen, die sie nicht installieren oder im Netzwerk benutzen sollten. Jeder Benutzer, der die Risiken seiner Handlungen auf dem Computer versteht, wird sich vernünftig verhalten und Malware aus dem Weg gehen.

Schließlich müssen Sie dafür sorgen, dass die Benutzer regelmäßig ihre Anti-Malware-Software starten. Am besten planen Sie deren Ausführung zusammen mit dem Benutzer.

27.3.4 Firewalls

Firewalls sind für die Abwehr bösartiger Programme aus dem Internet unverzichtbar. Dabei handelt es sich um Geräte oder Programme, die ein internes Netzwerk vor unberechtigten Zugriffen auf das und aus dem Internet schützen. Hardware-Firewalls schützen Netzwerke unter Verwendung verschiedener Methoden, wie beispielsweise durch das Verbergen von IP-Adressen und die Blockierung von TCP/IP-Ports.

In Netzwerken kommen üblicherweise zwei Firewall-Typen zum Einsatz: Hardware-Firewalls, die oft in den Router integriert sind, und Software-Firewalls, die auf den einzelnen Computern laufen. Beide Firewall-Arten schützen Ihren Computer und Ihr Netzwerk und arbeiten dabei Hand in Hand. Werfen wir also einen genaueren Blick auf die Funktionen einer typischen Router-Firewall und auf die Software-Firewall Ihres Computers, um zu untersuchen, auf welche Weise diese Ihr Netzwerk und Ihre Rechner schützen.

Konfiguration der Hardware-Firewall

Die meisten kleineren Netzwerke verwenden eine Hardware-Firewall, die in den Router integriert ist, wie beispielsweise den in Abbildung 27.26 dargestellten ASUS-Router. Eine Hardware-Firewall schützt das LAN vor Bedrohungen durch die Außenwelt durch das Filtern von Paketen, die so Geräte im internen Netzwerk nicht erreichen können. Das haben Sie in Kapitel 21, *Das Internet*, bereits erfahren. Router können aber noch mehr. Auf der im Webbrowser aufgerufenen Konfigurationsseite können Sie die Hardware-Firewall konfigurieren (Abbildung 27.27). Sehen wir uns die verschiedenen Einstellungsmöglichkeiten einmal an.



Abb. 27.26: ASUS-Router mit integrierter Firewall

Abb. 27.27: Konfigurationsseite der Firewall

Die Hardware-Firewall schützt vor vielen der üblichen Gefahren – Sie brauchen Sie nur einzuschalten. Jedes einzelne eingehende Datenpaket wird von der Firewall untersucht (*Stateful Packet Inspection*, SPI, siehe Abbildung 27.28). Durch SPI wird außerdem Datenverkehr blockiert, der nicht als Antwort auf ausgehenden Datenverkehr erkennbar ist. Sie können einzelne Ports auch komplett deaktivieren und damit sämtlichen ein- und ausgehenden Datenverkehr blockieren. Wie können externe Benutzer dann auf einen Webserver im LAN zugreifen? Da NAT die tatsächliche IP-Adresse des Servers verbirgt (wie in Kapitel 21 beschrieben), ist ein Mechanismus erforderlich, der eingehenden Datenverkehr akzeptiert und an den entsprechenden Computer weiterleitet.

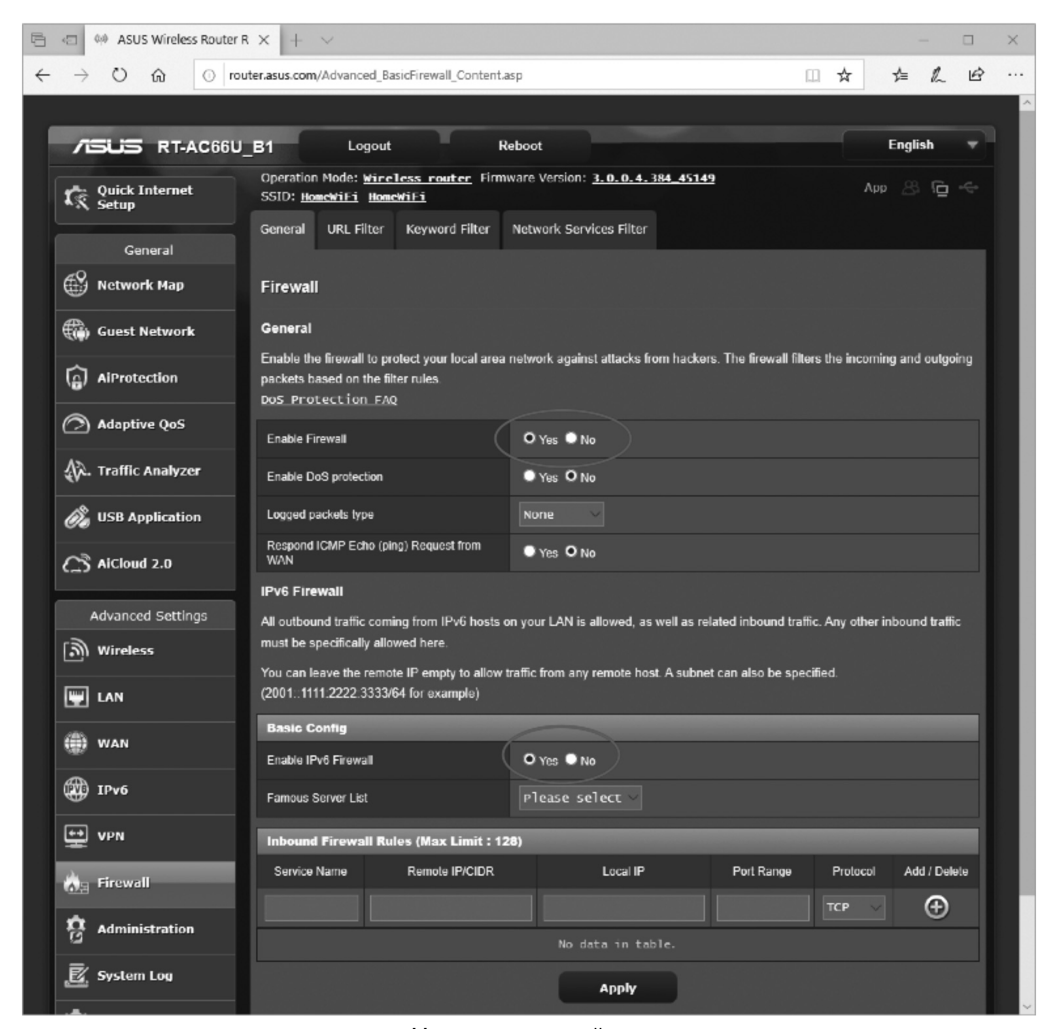


Abb. 27.28: SPI-Einstellungen

Die *Portweiterleitung* (*Port Forwarding*) gestattet es, in der Firewall einen Port zu öffnen und darauf eingehenden Datenverkehr an eine bestimmte IP-Adresse im LAN weiterzuleiten. Im Fall des eben erwähnten Webservers würden Sie Port 80 (für HTTP-Datenpakete) öffnen und den Router anweisen, den eingehenden Datenverkehr an den Server weiterzuleiten. Abbildung 27.29 zeigt die Konfiguration einer Portweiterleitung für HTTP-Pakete an einen internen Webserver.

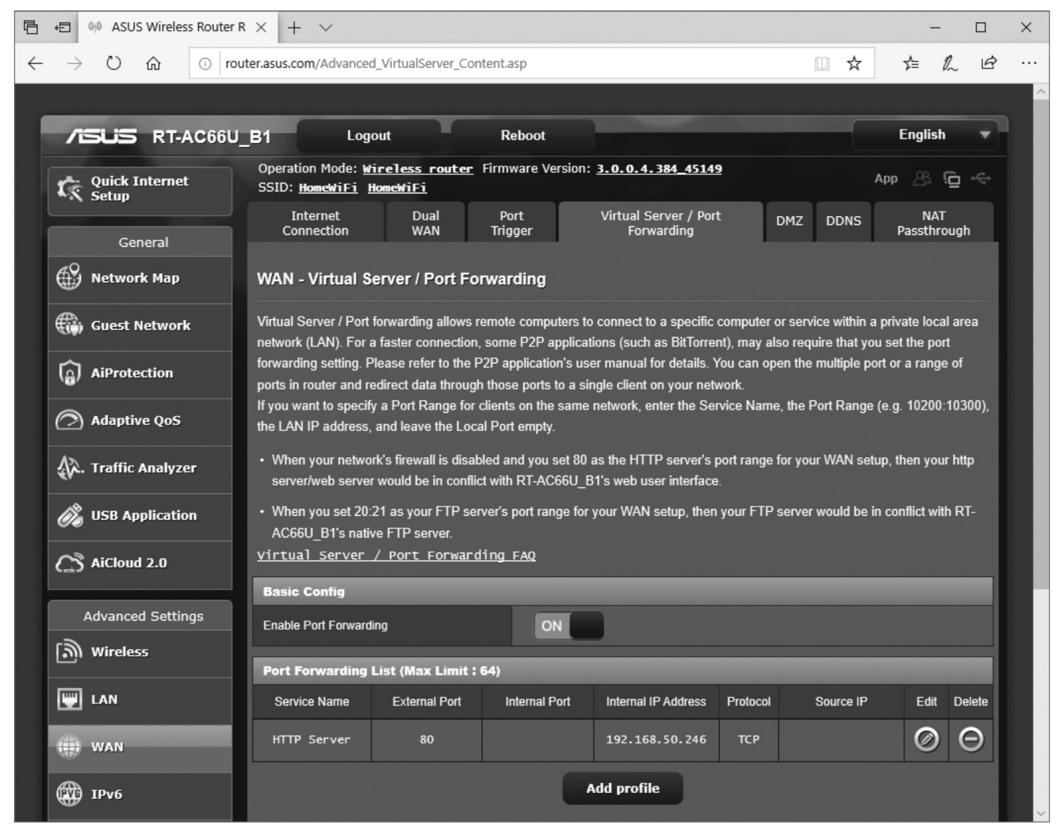


Abb. 27.29: Portweiterleitung

Portweiterleitungen sind aber nicht die einzige Möglichkeit, um in der Firewall Ports zu öffnen. Mittels *Port-Triggering* ist es möglich, anhand einer speziellen ausgehenden Verbindung automatisch einen Port für eingehende Verbindungen zu einem bestimmten Computer zu öffnen. Der Trigger-Port legt dabei die ausgehende Verbindung fest und der Zielport die eingehende Verbindung. Wenn Sie beispielsweise als Trigger-Port 3434 einstellen und den Zielport auf 1234 setzen, sorgt ausgehender Datenverkehr auf Port 3434 dafür, dass der Router den Port 1234 für eingehende Verbindungen öffnet und dort eingehenden Datenverkehr an den Computer zurückleitet, der den ausgehenden Datenverkehr auf Port 3434 verursacht hat. In Abbildung 27.30 sehen Sie die Konfiguration eines Routers, bei dem Port-Triggering für *IRC* (*Internet Relay Chat*) eingerichtet ist.

Falls Sie mehr als nur Portweiterleitung und Port-Triggering verwenden möchten und alle Ports eines Computers erreichbar sein sollen, benötigen Sie eine *DMZ* (Demilitarisierte Zone). Alle einer DMZ zugeordneten IP-Adressen sind nicht durch die Firewall geschützt und sämtliche Ports sind für eingehende Verbindungen zugänglich (Abbildung 27.31). Falls Sie nun denken, dass sich das ungeheuer gefährlich anhört, liegen Sie richtig! Ein PC in der DMZ ist sämtlichen Angriffen aus dem Internet ungeschützt ausgesetzt. Verwenden Sie die DMZ besser nicht!

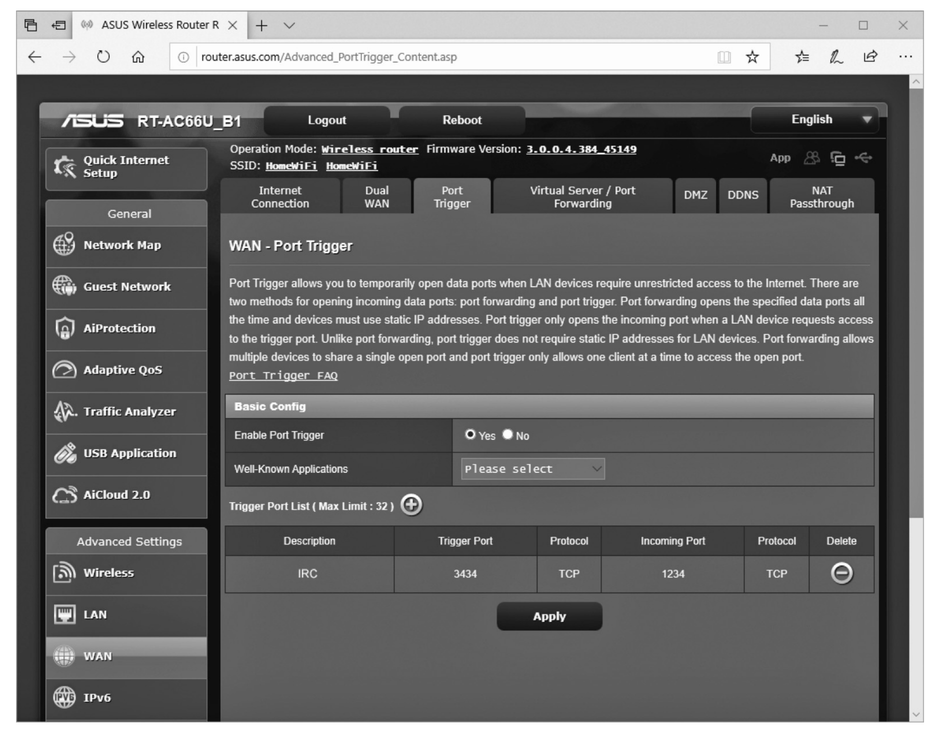


Abb. 27.30: Port-Triggering

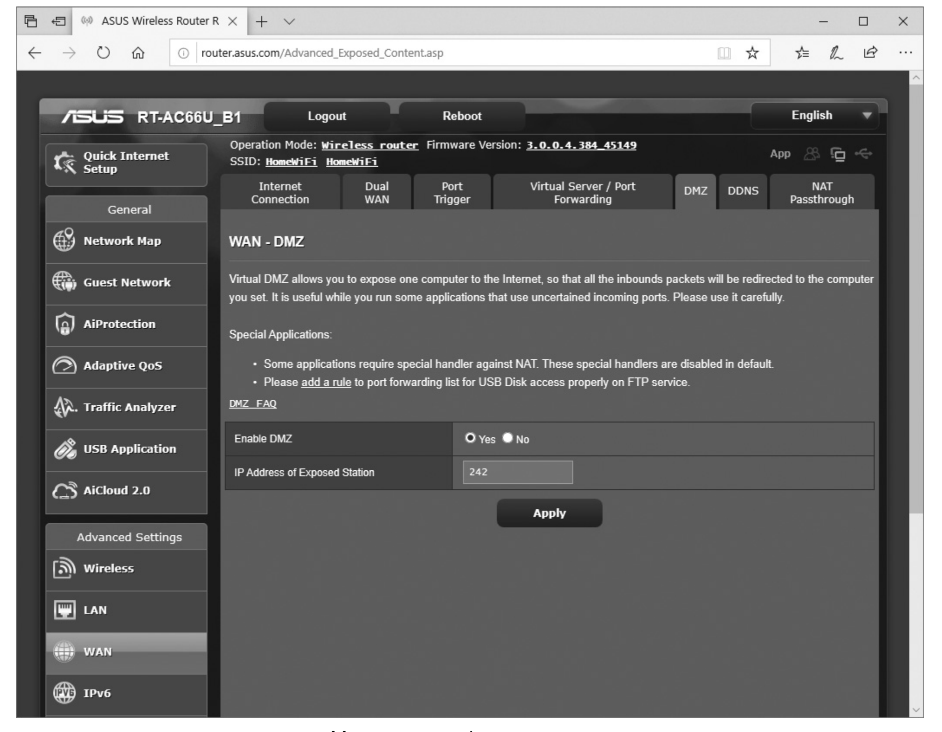


Abb. 27.31: Einrichtung einer DMZ

Software-Firewalls

Eine Hardware-Firewall bietet schon einen guten Schutz vor Angreifern aus dem Internet, Sie sollten aber auch eine Software-Firewall nutzen, z.B. die in Windows eingebaute, die den sinnigen Namen *Windows Defender Firewall* trägt (oder Windows Defender Firewall mit erweiterter Sicherheit). Die Windows-Firewall übernimmt die Schwerstarbeit beim Blockieren von Ports, der Protokollierung der Zugriffe und einiges mehr. Sie können in der Systemsteuerung auf die Windows-Firewall über das gleichnamige Applet zugreifen (Abbildung 27.32). Sie können die Windows-Firewall aktivieren oder deaktivieren und auswählen, welche Programme und Dienste nicht blockiert werden, die sogenannten *Ausnahmen*. Wenn Sie beispielsweise einen *Minecraft*-Server betreiben möchten (ein Computerspiel, das eine Internetverbindung benötigt), müssten Sie es in die Liste der Ausnahmen aufnehmen. Die meisten Programme fügen sich bei der Installation selbst dieser Liste hinzu, ansonsten erkundigt sich die Windows Defender Firewall bei der ersten Verwendung, ob Sie das fragliche Programm in die Liste der Ausnahmen aufnehmen möchten.

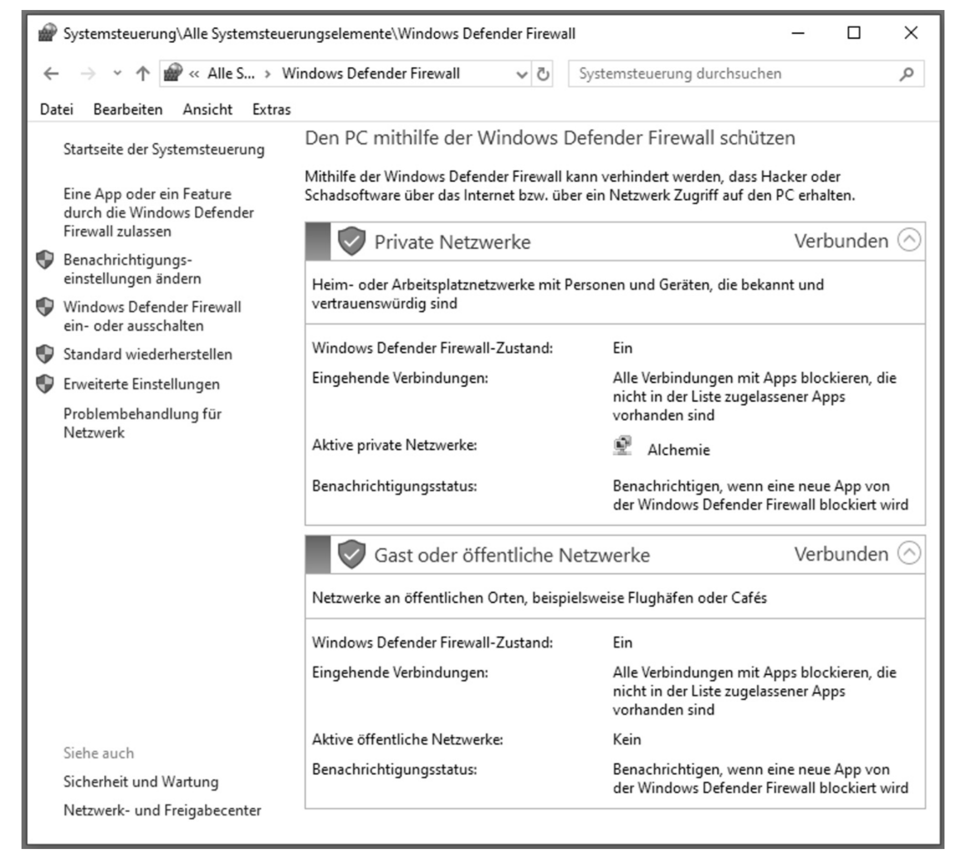


Abb. 27.32: Einstellungen der Firewall in Windows 10

Wichtig

Um die Windows-Firewall abzuschalten (was ich Ihnen nicht empfehlen kann), müssen Sie das Applet Windows-Firewall öffnen. Klicken Sie zunächst auf WINDOWS DEFENDER FIREWALL EIN- ODER AUSSCHALTEN und dann auf WINDOWS DEFENDER FIREWALL DEAKTIVIEREN (NICHT EMPFOHLEN). Sie müssen dies für jeden Netzwerktyp erledigen, den Sie verwenden.

Als Microsoft die Windows-Firewall zusammen mit Windows XP vorstellte, war der größte Nachteil die fehlende Berücksichtigung der Tatsache, dass ein einzelner PC, insbesondere ein tragbarer Computer, oft an verschiedene Netzwerke angeschlossen wird. Man möchte nun mal normalerweise nicht dieselben Firewall-Einstellungen für private und öffentliche Netzwerke verwenden. Microsoft musste daher einen Weg finden, um vertrauenswürdige Netzwerke (wie im Büro oder zu Hause) von nicht vertrauenswürdigen (wie dem öffentlichen WLAN-Zugang im Flughafen) zu unterscheiden. In nachfolgenden Windows-Versionen hat Microsoft daher drei Netzwerktypen festgelegt: DOMÄNENNETZWERK, PRIVATES NETZWERK und GAST ODER ÖFFENTLICHES NETZWERK.

- Ein *Domänennetzwerk* ist ein Windows-Netzwerk mit einem Domänen-Controller, auf dem ein Active-Directory-Dienst läuft. In diesem Fall teilt der Domänen-Controller Ihrem Computer mit, welche Freigaben erlaubt sind und welche nicht. Sie brauchen weiter nichts zu tun, wenn Sie einer Domäne beitreten.
- Ein *privates Netzwerk* ermöglicht es, Ressourcen freizugeben, andere Geräte im Netzwerk anzuzeigen, und gestattet es anderen Geräten, Ihren Computer im Netzwerk aufzufinden.
- Ein *öffentliches Netzwerk* sperrt alle Freigaben und deaktiviert die zum Auffinden Ihres Computers im Netzwerk erforderlichen Protokolle.

Wenn Ihr Computer sich erstmals mit einem Netzwerk verbindet, werden Sie dazu aufgefordert, einen Netzwerktyp anzugeben. Zur Auswahl stehen (in Windows 7) HEIMNETZWERK, ARBEITSPLATZNETZWERK und ÖFFENTLICHES NETZWERK. Windows 10 informiert darüber, dass Ihr PC im Netzwerk für andere Geräte sichtbar ist, wenn Sie nicht ÖFFENTLICH, sondern PRIVAT auswählen (Abbildung 27.33). Ihre Auswahl entscheidet darüber, ob Windows Freigaben erlaubt oder diese unterbindet.

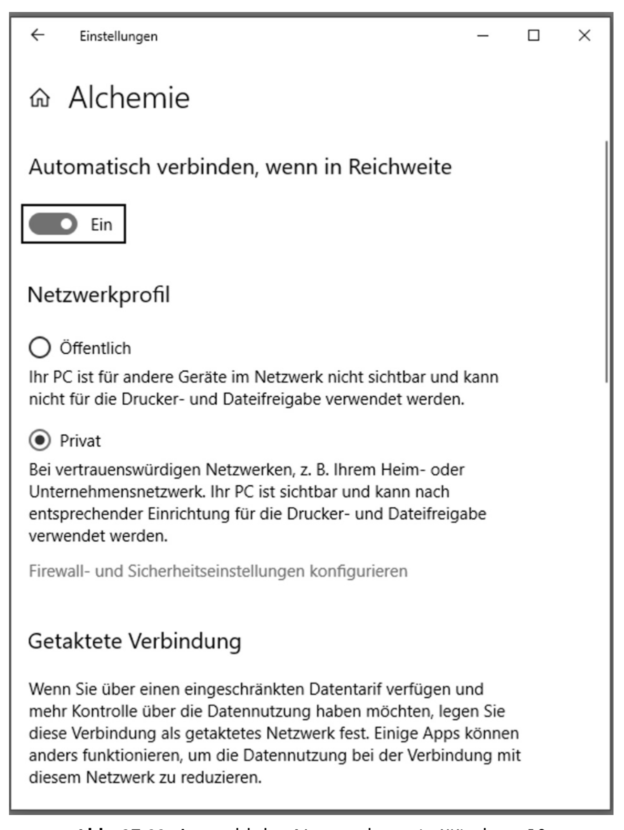


Abb. 27.33: Auswahl des Netzwerktyps in Windows 10

Wenn Ihr Computer einer Domäne beitritt, legt Windows den Netzwerktyp automatisch als Domänennetzwerk fest (sofern der Domänen-Controller keine gegenteilige Anweisung gibt, was aber unwahrscheinlich ist).

Wenn Sie sich in einem privaten Netzwerk (HEIMNETZWERK oder ARBEITSPLATZNETZWERK) befinden, erlaubt Windows das Auffinden Ihres Rechners und die Freigabe von Dateien und Druckern. In einem öffentlichen Netzwerk hingegen sind diese Ausnahmen nicht gestattet.

Wichtig

Die Einstellungen für die Netzwerkerkennung legen fest, ob ein Computer andere Geräte im Netzwerk auffinden kann (und umgekehrt). Aber auch bei aktivierter Netzwerkerkennung gibt es Firewall-Einstellungen, die bestimmte Verbindungen untersagen können.

Das wäre alles, solange Sie nur ein einziges Netzwerk nutzen. Aber was ist mit Computern (vornehmlich Laptops), die ständig an andere Netzwerke angeschlossen werden (Abbildung 27.34)? In diesem Fall sind für jedes Netzwerk eigene Firewall-Einstellungen erforderlich.



Abb. 27.34: Viele Computer benötigen mehr als eine Netzwerkeinstellung.

Um das zu unterstützen, erscheint das Dialogfeld zur Auswahl des Netzwerktyps jedes Mal, wenn Sie sich mit einem neuen Netzwerk verbinden. Darüber hinaus gibt es drei verschiedene Firewall-Einstellungen: eine für Domänennetzwerke, eine für private Netzwerke (HEIMNETZWERK oder ARBEITSPLATZNETZWERK) und eine für öffentliche Netzwerke.

Wichtig

Rechnen Sie in der CompTIA A+-Zertifizierungsprüfung mit Fragen, die sich auf private oder öffentliche Netzwerke beziehen. Merken Sie sich einfach nur, dass Sie Heim- und Arbeitsplatznetzwerken vertrauen dürfen, öffentlichen hingegen nicht.

Möglicherweise möchten Sie die Firewall-Einstellungen ändern, nachdem Sie den Netzwerktyp festgelegt haben. Wenn Sie dann im Applet WINDOWS DEFENDER FIREWALL die erweiterten Einstellungen aufrufen, stehen Ihnen viele weitere Konfigurationsmöglichkeiten zur Verfügung (Abbildung 27.35). Tatsächlich handelt es sich hier um ein komplett anderes Programm, nämlich um die WINDOWS DEFENDER FIREWALL MIT ERWEITERTER SICHERHEIT.

Die Windows-Firewall mit erweiterter Sicherheit ermöglicht eine viel genauere Kontrolle darüber, wie Windows Ausnahmen handhabt. Im normalen Applet WINDOWS DEFENDER FIREWALL können Sie nur ein Programm auswählen, es zu einer Ausnahme machen und die Blockade durch die Firewall aufheben. Nun verhält es sich aber so, dass Programme Netzwerkdaten sowohl empfangen als auch senden, und die einfache Windows-Firewall stellt kaum Möglichkeiten zur Verfügung, die Aspekte eingehender und ausgehender Verbindungen zu berücksichtigen. Die Windows Defender Firewall mit

erweiterter Sicherheit erweitert das Konzept der Ausnahmen um benutzerdefinierte Regeln für ein- und ausgehenden Datenverkehr. Abbildung 27.36 zeigt die Regeln für ausgehenden Datenverkehr eines typischen Windows-Systems.

Abb. 27.35: Windows-Firewall mit erweiterter Sicherheit

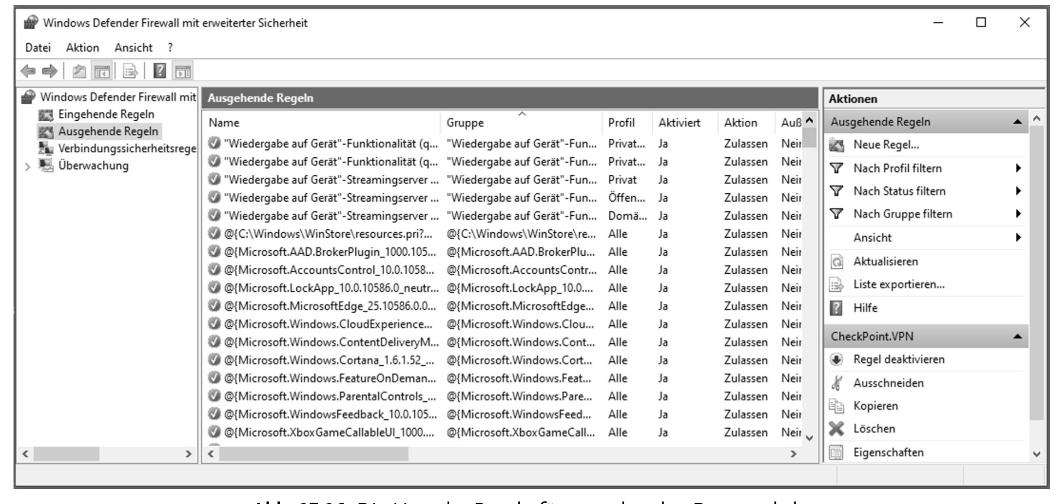


Abb. 27.36: Die Liste der Regeln für ausgehenden Datenverkehr

Zu einer Regel gehören mindestens folgende Dinge:

- Der Name des Programms
- Eine Gruppe, die zum Organisieren der Regeln dient
- Das zugehörige Profil (Jeder, Domäne, Öffentlich, Privat)
- Der Status (aktiviert oder deaktiviert)
- Entfernte und lokale Adresse
- Entfernte und lokale Portnummer

Sie können Regeln ganz nach Ihrem Geschmack hinzufügen, entfernen oder bearbeiten. Das wird jedoch schnell ziemlich kompliziert. Wenn Sie keinen guten Grund dafür haben, sehr viele Regeln anpassen zu müssen, dann bleiben Sie einfach bei der Standard-Firewall.

27.3.5 Internet-Appliances

Die Erläuterungen zu Firewalls kratzen kaum an der Oberfläche dessen, was es über aktive Netzwerkkomponenten zu sagen gäbe, die zum Schutz großer Netzwerke Verwendung finden. Unternehmensnetzwerke gehören im Allgemeinen nicht zum Aufgabenbereich A+-zertifizierter Techniker, dessen ungeachtet enthalten die Lernziele der CompTIA zwei Gerätetypen (IDS und IPS), die für die Sicherheit heutiger Netzwerke unverzichtbar sind, sowie das UMT-Konzept. Das sehen wir uns jetzt genauer an.

Ein *IDS* (*Intrusion Detection System*) ist ein Angriffserkennungssystem, das Datenpakete inspiziert und aktiv darüber wacht, dass niemand ins Netzwerk eindringt. Ein IDS kann im Netzwerk Bedrohungen erkennen, die einer Firewall entgehen, wie z.B. Viren, unzulässige Anmeldeversuche und andere wohlbekannte Angriffsformen. Und da nicht nur der externe Datenverkehr des Netzwerks überwacht wird, können auch interne Bedrohungen erkannt werden, beispielsweise die Aktivitäten eines auf einem USB-Speicherstick eingeschmuggelten Schwachstellenscanners, den ein verärgerter Mitarbeiter dazu verwendet, einen internen Datenbankserver anzugreifen.

Einem IDS steht immer irgendeine Möglichkeit zur Verfügung, den Netzwerkadministrator davon in Kenntnis zu setzen, dass ein Angriff stattfindet. Zum einen wird das natürlich protokolliert, viele Systeme bieten aber auch eine Benachrichtigung durch Pop-ups und den Versand einer E-Mail oder einer Textnachricht an. Darüber hinaus kann ein IDS auch auf entdeckte Angriffe reagieren. Es kann den Angriff zwar nicht selbst unterbinden, aber von anderen Geräten, die das können, Hilfe anfordern, etwa von der Firewall.

Ein *IPS* (*Intrusion Prevention System*) ähnelt einem IDS, nimmt aber unmittelbar am Datenverkehr teil. Diese aktive Überwachung hat drei Dinge zur Folge: Erstens kann ein IPS einen Angriff stoppen, während er stattfindet – es ist nicht notwendig, Hilfe von anderen Geräten anzufordern. Zweitens wirkt sich ein IPS negativ auf die Bandbreite und Latenzzeiten aus. Drittens kann die Netzwerkverbindung ausfallen, wenn das IPS nicht funktioniert. Manche IPS können eingehende Datenpakete anhand IP-Adresse, Portnummer oder Anwendungstyp in Echtzeit filtern, einige können die Pakete dabei sogar reparieren.

So leistungsfähig und ausgeklügelt diese Geräte auch sind, sie bleiben doch nur einzelne Werkzeuge im Waffenarsenal, das zum Schutz von Netzwerken bereitsteht. Hier kommt *UMT* (*Unified Threat Management*) ins Spiel, ein Konzept, das verschiedene Sicherheitsaufgaben auf einer Plattform vereinen soll. Bei UTM wird eine herkömmliche Firewall mit anderen Sicherheitsfunktionen kombiniert, wie etwa IPS, VPN, Lastverteilung, Anti-Malware-Software und vielen anderen Funktionalitäten. Der UTM-Ansatz hilft dabei, robuste Sicherheitsfunktionen tief im Netzwerk zu verankern, um zu schützen, was wirklich wichtig ist: unsere Daten.

27.3.6 Authentifizierung und Verschlüsselung

Aus den bisherigen Kapiteln wissen Sie, dass die Authentifizierung mit Benutzername und Kennwort der erste Schritt zum Schutz Ihrer Daten ist. Wenn Sie es aber mit Netzwerken zu tun haben, dann geht es nicht mehr um einzelne Benutzer, die an einem Rechner sitzen und Daten eintippen. Sie greifen auf entfernte Ressourcen zu und übertragen Anmeldedaten über das Internet. Was lässt sich also unternehmen, damit Ihr Benutzername und Kennwort möglichst nicht abgefangen werden kann?

Firewalls leisten gute Arbeit bei der Überwachung der in das und aus dem Internet übertragenen Netzwerkdaten, aber sie sind machtlos gegen Hacker, die den Datenverkehr in den öffentlich zugänglichen Teilen des Internets beobachten, um Sicherheitslücken zu finden. Wenn sich ein Datenpaket erst einmal im Internet befindet, kann es jeder mit der richtigen Ausrüstung auffangen und ansehen. Die Pakete enthalten reichlich Kennwörter, Kontennamen und andere für Hacker interessante Informationen, mit deren Hilfe sie in Ihr Netzwerk eindringen könnten. Weil wir Hacker nicht daran hindern können, diese Pakete zu untersuchen, müssen wir Daten *verschlüsseln*, damit sie nicht mehr lesbar sind.

Die Verschlüsselung des Datenverkehrs erfolgt auf vielen verschiedenen Ebenen und ist keineswegs auf Internet-basierte Aktivitäten beschränkt. Und es gibt nicht nur viele verschiedene Ebenen der Verschlüsselung, sondern jede Verschlüsselungsebene unterstützt mehrere Standards und Optionen, was die Verschlüsselung zu einem der kompliziertesten Bereiche im Umgang mit Netzwerken macht. Sie müssen wissen, wo die Verschlüsselung eine Rolle spielt, welche Optionen zur Verfügung stehen und was Sie tun können, um Ihr Netzwerk zu schützen.

Netzwerkauthentifizierung

Haben Sie sich schon einmal überlegt, was passiert, wenn eine Person einen Benutzernamen und ein Kennwort für den Zugriff auf das Netzwerk eingibt, statt sich nur auf einer lokalen Maschine anzumelden? Was passiert, wenn diese *Netzwerkauthentifizierung* angefordert wird? Wenn Sie glauben, die vom Benutzer eingegebenen Daten (Benutzername und Passwort) werden an irgendeinen Server geschickt, der sie überprüft, dann haben Sie recht – aber wissen Sie, wie Benutzername und Kennwort zu diesem System übertragen werden? Hier spielt die Verschlüsselung bei der Authentifizierung eine wichtige Rolle.

In einem LAN ist üblicherweise das Betriebssystem für die Authentifizierung und Verschlüsselung zuständig. In den heute bunt gemischten und immer stärker vernetzten Netzwerkumgebungen ist es wünschenswert, dass Betriebssysteme beliebige Clients anderer Betriebssysteme authentifizieren können. Moderne Betriebssysteme wie beispielsweise Windows und macOS verwenden bei der Authentifizierung standardisierte Verschlüsselungsverfahren wie z.B. *Kerberos* vom MIT, um unterschiedlichen Servern die Authentifizierung verschiedenartiger Clients zu ermöglichen. Diese LAN-Authentifizierungsverfahren sind üblicherweise transparent und funktionieren auch in heterogenen Netzwerken sehr gut.

Datenverschlüsselung

Verschlüsselungsverfahren bleiben nicht auf die Authentifizierungsebene beschränkt. Es gibt viele Möglichkeiten, auch Netzwerk*daten* zu verschlüsseln. Die Auswahl des Verschlüsselungsverfahrens ist weitgehend von der von dem Kommunikationssystem verwendeten Methode abhängig, über das eine Verbindung hergestellt wird. Viele Netzwerke bestehen aus mehreren über irgendeine Art privater Verbindung (normalerweise eine Telefonleitung wie etwa ISDN oder DSL) miteinander verknüpften Netzwerken. Das Verschlüsselungsverfahren, das Microsoft für derartige Netzwerke verwendet, ist *IPSec* (abgeleitet von *IP Security*). IPSec sorgt für die transparente Verschlüsselung zwischen Server und Client.

IPSec funktioniert auch in VPNs, aber hier werden üblicherweise andere Verschlüsselungsverfahren verwendet. Wenn Sie mit einem nicht vertrauenswürdigen Netzwerk verbunden sind, können Sie Ihren Datenverkehr schützen, indem Sie ihn durch einen VPN-Tunnel leiten. Sicherheitsbewusste Unternehmen verlangen oftmals sogar, dass alle mobilen Geräte über eine VPN-Verbindung mit einer Firmenniederlassung auf das Internet zugreifen.

Anwendungsverschlüsselung

Bei der Verschlüsselung können sogar TCP/IP-Anwendungen eine wichtige Rolle spielen. Bei der bekanntesten Anwendungsverschlüsselung handelt es sich um das Sicherheitsprotokoll *Secure Sockets Layer* (*SSL*), mit dem sichere Websites erstellt wurden. Heutzutage verwenden alle HTTPS (HTTP über TLS), das auf TLS (Transport Layer Security) beruht. Mit diesen Protokollen können Sie sichere Websites für Einkäufe über das Internet erstellen. HTTPS-Websites sind am `https://` in ihrer URL erkennbar (Abbildung 27.37).

Hinweis

HTTPS stand ursprünglich für HTTP über SSL, daher ergab das »S« am Ende einen Sinn. Inzwischen verwenden die meisten Websites das stabilere TLS zur Verschlüsselung der Verbindung. Man hat zwar stillschweigend SSL durch TLS ersetzt, aber auf ein neues Akronym wie »HTTPT« verzichtet.

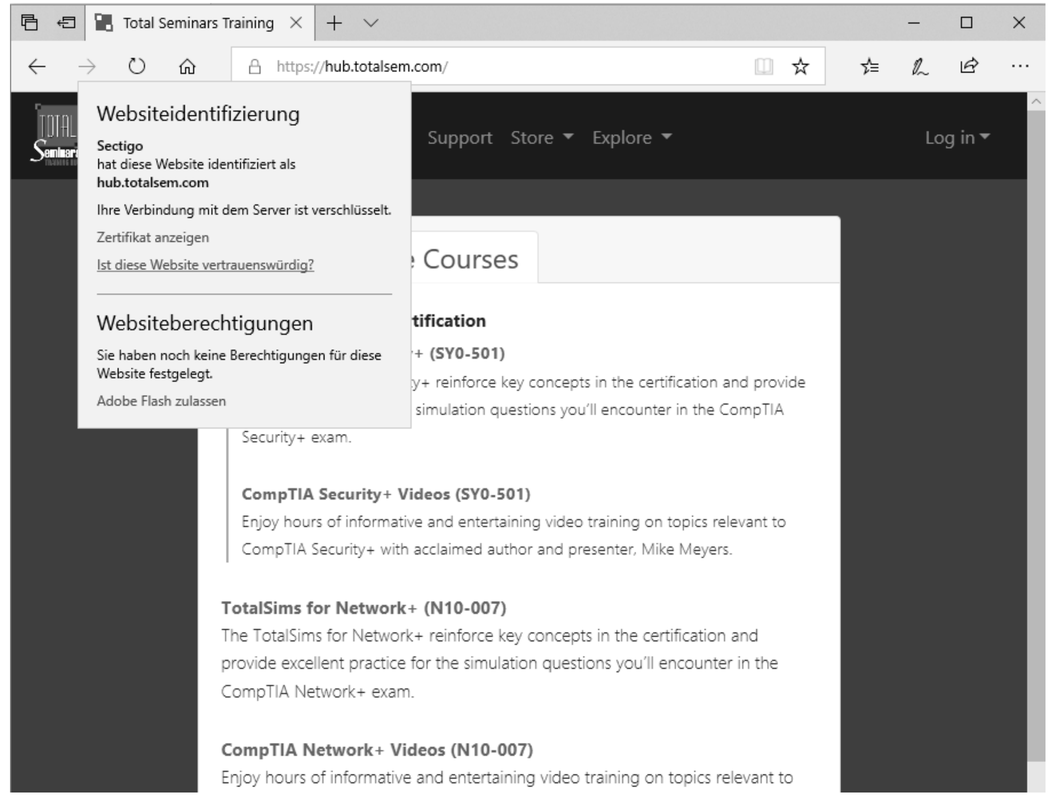


Abb. 27.37: Eine sichere Website

Wichtig

Bei vielen Appliances kommen kontextbasierte Regelsätze namens *DLP* (*Data Loss Prevention*, Schutz vor Datenverlust) zum Einsatz, die den Unternehmen dabei helfen sollen, das versehentliche Bekanntwerden von Daten zu verhindern. Die ausgehenden Datenpakete werden untersucht und der Datenstrom wird unterbrochen, sobald ein Regelverstoß festgestellt wird.

Um eine sichere Verbindung herzustellen, müssen Ihr Webbrowser und der Webserver ihre Daten verschlüsseln. Sowohl der Webserver als auch der Browser müssen die Daten des jeweils anderen also entschlüsseln können. Dazu sendet der Server einen öffentlichen Schlüssel zu Ihrem Webbrowser, damit dieser weiß, wie die eingehenden Daten zu entschlüsseln sind. Diese öffentlichen Schlüssel werden in Form eines *digitalen Zertifikats* gesendet. Dieses Zertifikat stellt nicht nur den öffentlichen Schlüssel bereit, sondern wurde auch von einer vertrauenswürdigen Organisation (einer *Certificate Authority*, oder kurz CA) signiert, die dafür bürgt, dass der empfangene öffentliche Schlüssel wirklich von dem Webserver stammt, und nicht etwa von irgendeiner böswilligen Person, die sich für diesen Webserver ausgibt. Es gibt eine ganze Reihe von Unternehmen, die digitale Zertifikate für Websites ausstellen, wie z.B. Symantec (ehemals VeriSign), Comodo und viele andere.

Ihr Webbrowser enthält eine integrierte Liste vertrauenswürdiger Organisationen. Wenn ein Zertifikat von einer Website eintrifft, das von einem dieser angesehenen Unternehmen signiert wurde, geschieht innerhalb des Browsers weiter gar nichts. Sie gelangen einfach auf die sichere Website und in einer Ecke Ihres Browsers wird ein kleines Schlosssymbol angezeigt. Abbildung 27.38 zeigt die integrierte Liste der vertrauenswürdigen Organisationen des Webbrowsers Firefox.

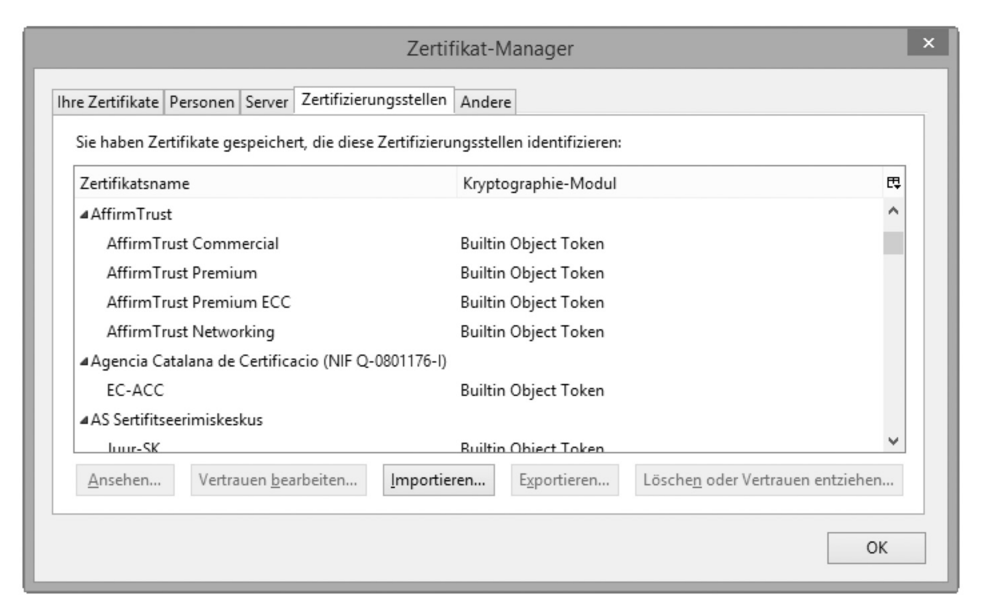


Abb. 27.38: Vertrauenswürdige Zertifizierungsstellen

Wenn Sie aber ein Zertifikat von Zertifizierungsstellen erhalten, die *nicht* in der Liste Ihres Browsers enthalten sind, oder wenn ein Zertifikat abgelaufen ist, dann wird eine Warnmeldung im Browser angezeigt. Dann können Sie entscheiden, ob Sie das Zertifikat dennoch akzeptieren und fortfahren wollen (Abbildung 27.39).

Was Sie jetzt tun, bleibt Ihnen überlassen. Wollen Sie diesem Zertifikat trauen? Normalerweise sollten Sie die Warnung des Browsers beachten und seiner Empfehlung folgen. Die Gründe für ungültige Zertifikate sind meistens ziemlich langweilig. Häufig hat der Websitebetreiber einfach nur vergessen, sie zu aktualisieren. Ein ungültiges Zertifikat kann aber sehr wohl darauf hinweisen, dass eine Website oder die Verbindung mit ihr kompromittiert wurde! Fügen Sie nur dann eine Ausnahme hinzu, wenn Sie *wissen*, dass der Besuch der Website sicher ist. Es könnte beispielsweise erforderlich sein, eine Ausnahme hinzuzufügen, um auf einen Webserver im Intranet Ihres Unternehmens zugreifen zu können.

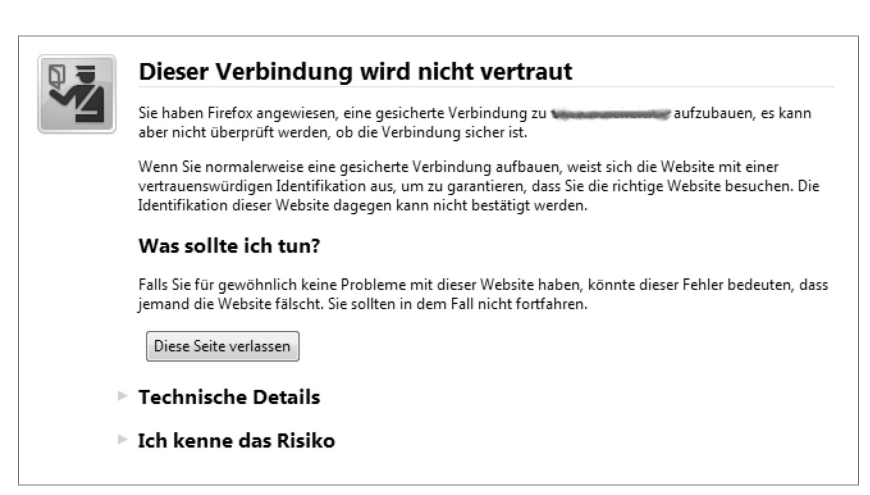


Abb. 27.39: Firefox kann nicht feststellen, ob eine Verbindung sicher ist.

27.3.7 Besondere Aspekte bei drahtlosen Netzwerken

Wie Sie aus Kapitel 20 bereits wissen, bereiten drahtlose Netzwerke (WLANs) Technikern zusätzliche Kopfschmerzen hinsichtlich ihrer Sicherheit. Hier sind einige der Punkte, die es zu beachten gilt:

- Aktivieren Sie ein Verschlüsselungsverfahren, mindestens WPA oder besser das sicherere WPA2 oder WPA3 und konfigurieren Sie die Clients entsprechend.
- Deaktivieren Sie DHCP und verlangen Sie von WLAN-Clients die Verwendung statischer IP-Adressen.
- Wenn Sie DHCP verwenden müssen, richten Sie nur die in Ihrem Netzwerk benötigten DHCP-Adressen ein, um ungenutzte Funkverbindungen zu vermeiden.
- Ändern Sie die Standardeinstellung der SSID bei den Zugangspunkten.
- Filtern Sie nach MAC-Adressen, um nur bekannten Clients Zugang zum Netzwerk zu gewähren.
- Ändern Sie Standardbenutzernamen und Kennwörter der WLAN-Zugangspunkte. Selbst wenn sie sicher aussehen, könnte bekannt sein, wie sie erzeugt werden.
- Aktualisieren Sie gegebenenfalls die Firmware.
- Sorgen Sie dafür, dass die Firewall-Einstellungen der Zugangspunkte aktiviert sind (falls verfügbar).
- Konfigurieren Sie die NAT/DNAT-Einstellungen des Routers.
- Konfigurieren Sie Filterregeln und Kindersicherung.
- Schenken Sie auch der physischen Sicherheit des Routers Beachtung.

27.4 Wiederholung

27.4.1 Fragen

1. Wie nennt man die Manipulation von Menschen, um Zugriff auf Netzwerkressourcen zu erhalten?
   A. Cracking
   B. Hacking
   C. Netzwerk Engineering
   D. Social Engineering

2. Womit ist eine sichere Hardware-Authentifizierung möglich?
   A. Sichere Kennwörter
   B. Verschlüsselte Kennwörter
   C. NTFS
   D. Smartcards
3. Mit welchem der folgenden Hilfsprogramme lässt sich verhindern, dass sich ein Benutzer bei einem lokalen Rechner anmeldet, ihm aber weiterhin die Anmeldung bei der Domäne gestattet ist?
   A. AD-Richtlinien
   B. Gruppenrichtlinien
   C. Lokale Sicherheitsrichtlinie
   D. Benutzereinstellungen
4. Welche Funktion einer Hardware-Firewall ermöglicht es, dass auf einem bestimmten Port eingehender Datenverkehr eine IP-Adresse im LAN erreicht?
   A. Portweiterleitung
   B. NAT
   C. DMZ
   D. Mehrfaktor-Authentifizierung
5. Klaus hat ein Spiel aus dem Internet heruntergeladen und installiert. Als er es startet, wird ein Blue Screen angezeigt. Nach dem Neustart des Rechners entdeckt er, dass der Ordner mit seinen eigenen Dokumenten gelöscht wurde. Was ist geschehen?
   A. Er hat ein Spyware-Programm installiert.
   B. Er hat einen Trojaner installiert.
   C. Er hat gegen die Gruppenrichtlinien verstoßen.
   D. Er hat gegen die lokale Sicherheitsrichtlinie verstoßen.
6. Was sollte Maria bei ihrem WLAN-Router aktivieren, um ihn möglichst sicher zu machen?
   A. NTFS
   B. WEP
   C. WPA
   D. WPA2
7. Welches Werkzeug würden Sie zur Aktivierung von Überwachungsfunktionen auf lokaler Ebene verwenden?
   A. AD-Richtlinien
   B. Gruppenrichtlinien
   C. Lokale Sicherheitsrichtlinie
   D. Benutzereinstellungen
8. Johannes hat sich eine falsche Uniform besorgt und sich als Wachmann eines Unternehmens verkleidet, um dann zusammen mit echten Angestellten das Firmengelände zu betreten und sich Zugang zu den Ressourcen des Unternehmens zu verschaffen. Wie werden derartige Angriffe genannt?
   A. Administrativer Zugriff
   B. Datenvernichtung
   C. Spoofing
   D. Tailgating

9. An Ihrem ersten Arbeitstag erhält Alexandra ein Arbeitsblatt, auf dem die für Benutzer genehmigten Programme und klare Anweisungen zu finden sind, die den Einsatz anderer Programme verbieten. Welche Art von Regeln muss sie hier befolgen?
   A. Klassifizierung
   B. Konformität
   C. Gruppe
   D. Sicherheit
10. Melanie will in ihrem Unternehmen Richtlinien durchsetzen, um Infektionen mit Malware zu verhindern oder zumindest zu beschränken. Welche Richtlinie wäre die beste Lösung?
   A. Anti-Malware-Software auf allen Rechnern installieren. Anwender schulen, damit sie wissen, wie sie diese benutzen können.
   B. Anti-Malware-Software auf allen Rechnern installieren. Die Software für regelmäßige Scans einrichten.
   C. Anti-Malware-Software auf allen Rechnern installieren. Die automatische Aktualisierung aktivieren und die Software für regelmäßige Scans einrichten.
   D. Anti-Malware-Software auf allen Rechnern installieren. Die automatische Aktualisierung aktivieren und die Software für regelmäßige Scans einrichten. Die Anwender schulen, damit sie wissen, welche Websites und Downloads sie meiden sollten.

27.4.2 Antworten

1. **D.** Beim Social Engineering werden Menschen benutzt oder manipuliert, um Zugang zu Netzwerkressourcen zu erhalten.
2. **D.** Smartcards sind ein Beispiel für Geräte zur Hardwareauthentifizierung.
3. **C.** Über die lokale Sicherheitsrichtlinie können Sie verhindern, dass sich jemand bei einem lokalen Rechner anmeldet.
4. **A.** Verwenden Sie die Portweiterleitung, um einen Port der Firewall zu öffnen und eingehenden Datenverkehr an einen bestimmten Rechner weiterzuleiten.
5. **B.** Klaus hat offensichtlich einen Trojaner installiert, eine Malware, die sich als Spiel getarnt hat.
6. **D.** Maria sollte WPA2 bei ihrem WLAN-Router einrichten und aktivieren.
7. **C.** Die lokalen Überwachungsfunktionen können Sie über die lokale Sicherheitsrichtlinie aktivieren.
8. **D.** Johannes hat sich im Schlepptau echter Beschäftigter bei dem nichts ahnenden Unternehmen unberechtigt Zutritt verschafft. Diese Vorgehensweise wird Tailgating genannt.
9. **B.** Alexandra muss Konformitätsregeln befolgen, damit die Anzahl der Anrufe beim technischen Support minimiert und die Verfügbarkeit der Rechner und Server im Unternehmen maximiert wird.
10. **D.** Die beste Richtlinie umfasst die Aktivierung der automatischen Aktualisierung, regelmäßige Scans und die Schulung der Anwender.

Betriebsabläufe 28

Themen in diesem Kapitel:

- Richtlinien für die verschiedenen Formen der Dokumentation
- Änderungsmanagement richtig implementieren
- Katastrophenvorbeugung und Wiederherstellung richtig implementieren

Der Begriff *Betriebsabläufe* umfasst für jede Organisation eine ganze Menge: Sicherheitsrichtlinien (Kapitel 1, *Sicherheit und Professionalität*), die Beachtung von Umweltschutzbestimmungen (Kapitel 27, *Computersicherheit*), Unternehmensrichtlinien zum Umgang mit illegalen Inhalten oder Handlungen (auch Kapitel 27) und verbindliche Kommunikation und professionelles Auftreten (wieder Kapitel 1), Dinge, die jeder Techniker beherrschen sollte. Darüber hinaus kommen in der CompTIA A+-Prüfung 1002 noch die Grundlagen der Skript-Erstellung (Kapitel 15, *Eingabeaufforderung*) und Technologien für den Fernzugriff (Kapitel 21, *Das Internet*) hinzu.

Dieses Kapitel wirft einen Blick auf einen weiteren Aspekt der Betriebsabläufe, nämlich auf ein Geschäftsgebaren, das *Kontinuität* ermöglicht. Das ist im Grunde genommen nur ein hochtrabender Ausdruck dafür, dass ein Unternehmen oder eine Organisation sowohl bei alltäglichen Änderungen als auch im Katastrophenfall mehr oder weniger gleich vorgehen sollte. Wir konzentrieren uns bei der Geschäftskontinuität und den Betriebsabläufen auf drei Kategorien: Dokumentation, Änderungsmanagement sowie Katastrophenvorbeugung und Wiederherstellung.

1002

28.1 Richtlinien für die Dokumentation

Für die Erhaltung der Kontinuität und der Struktur einer Organisation ist eine Dokumentation erforderlich. Dokumentationen gibt es in den verschiedensten Formen, aber für einen angehenden Techniker sind vor allem drei Kategorien von Belang: Netzwerkdokumentation, Unternehmensrichtlinien und Bestandsverwaltung.

28.1.1 Netzwerkdokumentation

Netzwerkdokumentation ist ein Plan der Netzwerkkonfiguration einer Organisation und der Topologie dieses Netzwerks für heutige und zukünftige Techniker, die das Netzwerk ändern oder reparieren müssen. Für das Netzwerk insgesamt sind größtenteils Systemadministratoren und CompTIA Network+-Techniker verantwortlich, die eigentliche Umsetzung von Reparaturen obliegt aber häufig CompTIA A+-Technikern. Sie müssen Netzwerktopologiediagramme lesen können, auf die Wissensdatenbank des Unternehmens und interne Artikel zugreifen, sowie Zwischenfallberichte erstellen, wenn es zu Problemen kommt.

Netzwerktopologie-Diagramme

Ein *Netzwerktopologie-Diagramm* beschreibt den Aufbau eines Netzwerks. Dazu gehören Switches, Router, WAPs, Server und Arbeitsplatzrechner (Abbildung 28.1). Komplexere Diagramme geben zudem Verbindungstypen und -geschwindigkeiten sowie die verwendeten Technologien an (beispielsweise wird ein WAP als 802.11ac AC2600 gekennzeichnet). Häufig kommt dabei die Symbolsammlung von Cisco zum Einsatz, die beim Erstellen dieser Diagramme eine große Hilfe ist (Abbildung 28.2).

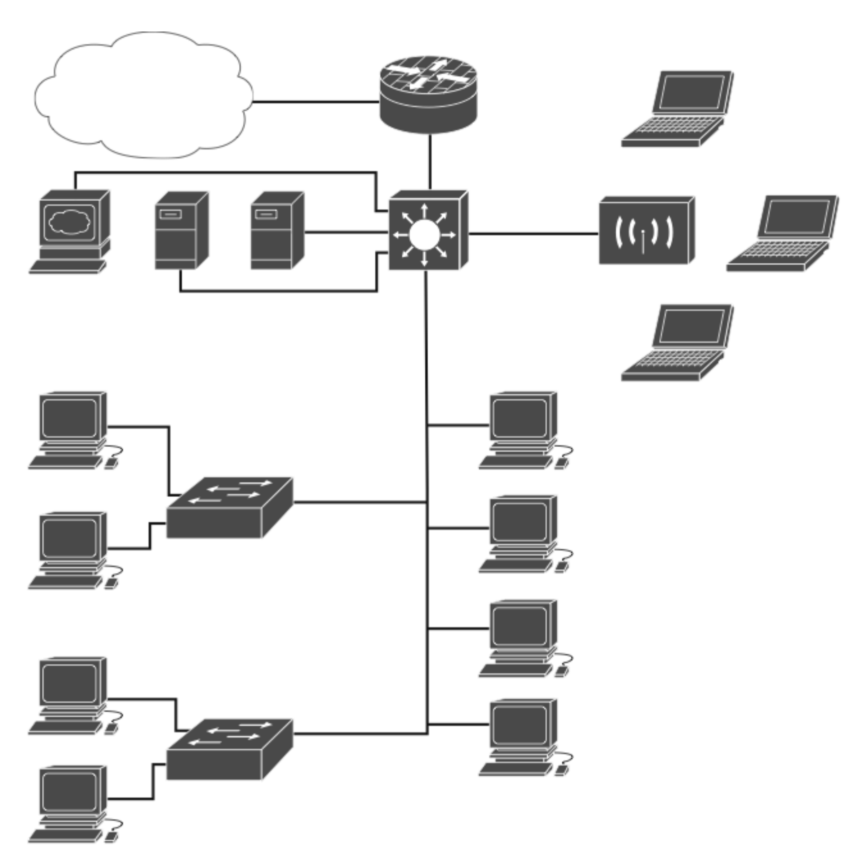


Abb. 28.1: Typisches Netzwerktopologie-Diagramm

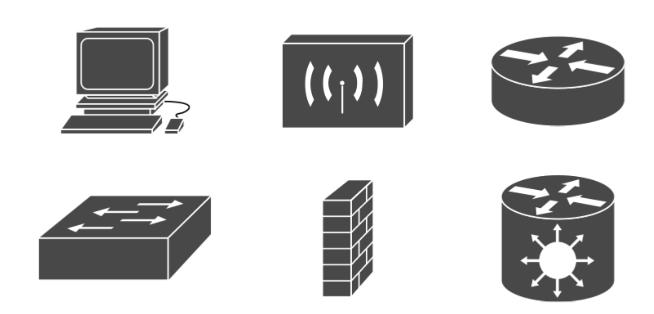


Abb. 28.2: Einige Beispiel aus der Symbolsammlung von Cisco

Wissensdatenbank/interne Artikel

Die Dokumentation soll die Zusammenarbeit von Angestellten untereinander und von verschiedenen Abteilungen ermöglichen und koordinieren. Zu diesem Zweck wird eine *Wissensdatenbank* erstellt und gepflegt, in der Informationen über alle vorhandenen Geräte sowie aufgetretene Probleme und deren Lösung gespeichert werden. Sie ist für heutige und zukünftige Techniker ein unverzichtbares Werkzeug. Die internen Artikel dokumentieren Details der im Unternehmen eingesetzten Technik und enthalten unter anderem Links zu den Websites der Hersteller und weitere Informationen.

Zwischenfallberichte

Die Dokumentation bestimmter Probleme durch Zwischenfallberichte erleichtert heutigen und zukünftigen Technikern den Umgang mit problematischer Hardware und bestimmten Einzelpersonen. Wenn es beispielsweise in fünf verschiedenen Abteilungen identische Farblaserdrucker gibt und bei einem davon nach dem Drucken von 10.000 Seiten regelmäßig Papierstaus auftreten, sollten Sie das Problem – den Zwischenfall – und die Lösung dokumentieren. Das ist ein deutlicher Hinweis darauf, dass es bei den anderen vier Druckern potenziell zu Problemen kommen kann, wenn sie ebenso intensiv genutzt werden.

28.1.2 Unternehmensrichtlinien

Die für Mitarbeiter geltenden Ziele und Regeln sollen den Gewinn des Unternehmens steigern und für die Einhaltung gesetzlicher Vorschriften sorgen. Zu diesen *Unternehmensrichtlinien* gehören neben der Einhaltung gesetzlicher Vorschriften unter anderem auch Nutzungsbedingungen für firmeneigene Geräte und Richtlinien für Kennwörter.

Erfüllung gesetzlicher Auflagen

Es gehört zu den Aufgaben einer Regierung, sichere Arbeitsumgebungen zu gewährleisten und die Ausbeutung von Arbeitern zu minimieren. Zu diesem Zweck werden Regeln und Vorschriften entwickelt, die festlegen, wie mit Arbeitsplätzen, Mitarbeitern und Arbeitsmaterial verfahren werden *sollte*. Vernünftig geführte Unternehmen sorgen für die Erfüllung gesetzlicher Auflagen – die Einhaltung der Regeln und Vorschriften –, um die Gesundheit der Belegschaft zu wahren.

Nutzungsbedingungen

Die *Nutzungsbedinungen* beschreiben, was ein Angestellter mit unternehmenseigen Geräten anfangen darf und was nicht. Ein firmeneigener Laptop darf beispielsweise nur für geschäftliche Zwecke eingesetzt werden. Die Nutzungsbedingungen könnten es den Angestellten auch untersagen, von unternehmenseigenen Computern aus auf illegale Websites zuzugreifen. Die Nutzungsbedingungen sind oft sehr detailliert und müssen von den Angestellten schriftlich akzeptiert werden.

Kennwörter

Wir haben uns in Kapitel 13 bereits mit Richtlinien für Kennwörter befasst, deshalb möchte ich an dieser Stelle nur hinzufügen, dass in vielen Unternehmen detaillierte Kennwortrichtlinien gelten, die so ziemlich jeden Aspekt betreffen, wie die Angestellten Benutzerkonten und Zugangsdaten einrichten und verwenden müssen. Eine ausführliche *Kennwortrichtlinie* könnte beispielsweise Folgendes beinhalten: wie lang und komplex ein Kennwort sein muss, aus welchen Zeichen es zusammengesetzt ist, wann Multifaktor-Authentifizierung verwendet werden muss, ob Kennwörter ablaufen (und wenn ja, wie oft), ob ein BIOS-Kennwort vergeben werden muss und sogar, was Sie tun sollten, wenn ein Vorgesetzter verlangt, dass Sie ein Kennwort preisgeben!

28.1.3 Bestandsverwaltung

Mithilfe der *Bestandsverwaltung* helfen Techniker dabei, das Eigentum eines Unternehmens zu schützen. Dabei kommen unter anderem Barcodes und RFID-Etiketten zum Einsatz.

Barcodes

Auf vielen Bestandsartikeln befindet sich ein einfacher Aufkleber mit einem *Barcode*, einer eindeutigen Kombination aus Zeichen und Ziffern, die einen bestimmten Gegenstand identifiziert. Abbildung 28.3 zeigt einen solchen Aufkleber. Der Barcode dient als eine Art Fingerabdruck für einen Gegenstand und lässt sich leicht scannen. Barcodes haben den Nachteil, dass sie nur lesbar, aber nicht beschreibbar sind. Daten oder Informationen hinzuzufügen ist nicht möglich.



Abb. 28.3: Barcode auf einer SSD, der die Seriennummer codiert

RFID-Etiketten

RFID-Etiketten (*Radio Frequency Identification*, Funkfrequenzkennung) verwenden das gleichnamige drahtlose Netzwerkprotokoll zur Identifizierung (Abbildung 28.4). Das RFID-Etikett besteht aus einem Mikrochip und einer Antenne und kann auch ohne direkte Sichtverbindung mit einem RFID-Scanner ausgelesen werden. Die meisten RFID-Etiketten sind passiv. Das heißt, dass der RFID-Chip die benötigte Energie durch das Signal des Scanners erhält. Ein aktives RFID-Etikett hingegen verwendet eine Batterie oder eine externe Energiequelle, um Signale senden und empfangen zu können. Beide Typen lassen sich bei der Bestandsverwaltung einsetzen. Im Gegensatz zu Barcodes können die im RFID-Chip gespeicherten Daten aktualisiert werden.



Abb. 28.4: RFID-Etikett

28.2 Änderungsmanagement

CompTIA A+-Techniker sitzen beim Management der Infrastruktur in der ersten Reihe. Sie wissen, was funktioniert, was nicht funktioniert und was geändert werden muss. Die alten Laserdrucker in der Buchhaltung werden den Anforderungen der Benutzer beispielsweise schon länger nicht mehr gerecht und Sie verbringen jede Woche viel zu viel Zeit damit, sie am Laufen zu halten. Und Sie sind es auch leid, dass sich die Benutzer dauernd beklagen. Hier muss sich etwas ändern.

Änderungen werden nicht nur durch den tatsächlichen Bedarf verursacht, häufig werden sie auch von der Führungsebene veranlasst. Jeder erfahrene Techniker kann Ihnen von den Schwierigkeiten berichten, die mit großen Betriebssystemaktualisierungen einhergehen. Oder von dem lächerlich großen Arbeitsaufwand, eine betriebsnotwendige Anwendung zu upgraden oder eine neue, absolut unverzichtbare Anwendung einzuführen.

In jedem Betrieb gibt es formale und eher zwanglose Änderungsmanagementprozesse. Sie können beispielsweise nicht einfach einen neuen Laserdrucker kaufen, ohne sich über die Kosten und die Folgen Gedanken zu machen. Sie können auch nicht einfach das Betriebssystem von 100 Benutzern aktualisieren, ohne es vorher gründlich getestet zu haben. Sehen wir uns also einige dieser Prozesse und ihre Umsetzung an.

28.2.1 Änderungsmanagementprozesse

Ein *Änderungsmanagementprozess* ermöglicht es einem Unternehmen, Änderungen an der IT-Infrastruktur auf sichere und kostengünstige Weise vorzunehmen. Es gibt keinen allgemeingültigen Leitfaden für ein Änderungsmanagement, allerdings orientieren sich die meisten Unternehmen am gesunden Menschenverstand. Hier ist ein Abriss der von der CompTIA empfohlenen Vorgehensweise:

- Informieren Sie sich über dokumentierte Geschäftsprozesse.
- Ermitteln Sie den Zweck der Änderung.
- Finden Sie heraus, wie weitreichend die Änderung ist.
- Analysieren Sie, welche Risiken damit verbunden sind, die Änderung durchzuführen (oder es zu unterlassen).
- Planen Sie die Änderung.
- Informieren Sie die Benutzer über die Notwendigkeit, die Vorteile und die Kosten der Änderung.
- Stellen Sie ein eigenes Team für das Änderungsmanagement zusammen.
- Entwickeln Sie einen Ausfallplan für den Fall, dass die Änderung negative Folgen hat.
- Dokumentieren Sie alles sorgfältig.

28.2.2 Implementierung der Änderung (Fallbeispiel)

Ein Unternehmen, das einen Änderungsmanagementprozess umsetzen möchte, sollte Änderungen so gestalten, dass sie sich als klar und deutlich dokumentierte Geschäftsprozesse manifestieren. Zu Ihren Aufgaben als Techniker gehört es, dass Sie sich mit diesen Dokumenten vertraut machen, damit Sie den Prozess schon verstanden haben, wenn Sie mit den Änderungen in Berührung kommen. Wenn die Änderung umgesetzt wird, sollten Sie die dokumentierten Geschäftsprozesse nachlesen, damit Sie nicht peinlicherweise einen wichtigen Schritt übersehen.

Hier ist ein typisches Fallbeispiel für ein Änderungsmanagement. Julia von der *Bayland Widgets Corporation* möchte 16 Systeme im Entwicklungslabor von Windows 7 auf Windows 10 upgraden, weil die Benutzer nach einem neueren Betriebssystem verlangen.

Zweck der Änderung

Kein Unternehmen wird Ihnen gestatten, neue Geräte zu beschaffen oder Upgrades vorzunehmen, ohne zu wissen, weshalb das notwendig ist. Wenn Sie eine Änderung vorschlagen, sollten Sie den Zweck der Änderung dokumentieren. In Julias Fall haben die Benutzer nach dem neuesten Betriebssystem von Microsoft verlangt, um besser mit ihren Kunden zusammenarbeiten zu können, die alle zu Windows 10 gewechselt sind. Der Zweck der Änderung ist also, den Kunden bessere Leistungen und verbesserte Unterstützung bieten zu können.

Umfang der Änderung

Zusammen mit dem Zweck der Änderung legt der Umfang der Änderung fest, wer und was davon betroffen ist. Dazu gehört eine Bestandsliste der betroffenen Systeme, die Anzahl der Mitarbeiter, die an der Durchführung der Änderung beteiligt sind, die Zeit, die für die Änderung erforderlich ist, und häufig auch eine Abschätzung der Kosten, die mit der Änderung verbunden sind.

Im Entwicklungslabor sind 16 Geräte von der Änderung betroffen. (Die Kosten hängen davon ab, welche Edition von Windows 10 installiert wird: Home, Pro oder Enterprise.)

Risikoanalyse

Alle Änderungen an der Infrastruktur sind mit einem Risiko verbunden. Bei ordnungsgemäßem Änderungsmanagement ist eine *Risikoanalyse* erforderlich, die mögliche Probleme, die mit der Änderung einhergehen könnten, ausführlich beurteilt. Was ist, wenn das Upgrade fehlschlägt? Wurde die neue Anwendung auf einem Testsystem auf Herz und Nieren geprüft? Verfügen die neuen Computer über eine geeignete Firewall? Geraten Sie nicht in Panik (wenigsten nicht allzu sehr), denn jede Risikoanalyse wird aller Wahrscheinlichkeit nach bei einem für Sicherheitsfragen zuständigen Mitarbeiter landen – und diese Person ist möglicherweise sehr an Ihrer Meinung und Ihren Bedenken interessiert!

Für die Änderung planen

Was muss vor der Durchführung der Änderung unternommen werden? Was muss gekauft werden? Wo können neue, noch nicht installierte Geräte gelagert werden? An welchen Tagen wird die Änderung durchgeführt? Wie viel Zeit nimmt sie in Anspruch? Wer kann Sie vertreten, während Sie anderweitig beschäftigt sind? Alle Aufgaben, die erledigt sein müssen, bevor Julia loslegt, sind in einem *Plan für die Änderung* aufgeführt.

Benutzerakzeptanz

Zu einem erfolgreichen Änderungsmanagement gehört es auch, die Benutzer darüber zu informieren, weshalb die Änderung notwendig ist und wie sie mit dem veränderten System zurechtkommen. Die *Benutzerakzeptanz* ist für die erfolgreiche Umsetzung von Änderungen unverzichtbar. Das bedeutet insbesondere, dass Schulungen erforderlich sind. Wissen die Benutzer, wie sie die neuen Features des Druckers nutzen können? Welche neuen Funktionen des aktualisierten Betriebssystems sollten die Benutzer kennen? Kommen die Benutzer mit der neuen Anwendung gut zurecht? Und ist ihnen klar, dass sie die alte nicht mehr verwenden dürfen?

Änderungsausschuss

Julia hat also alles dokumentiert. Von wem sollte sie sich die Durchführung der Änderung genehmigen lassen? Dafür ist der *Änderungsausschuss* zuständig. Zum Änderungsausschuss gehören Techniker und Vertreter der Führungskräfte, der IT-Sicherheit und der Verwaltung, die sich regelmäßig treffen (üblicherweise vierteljährlich). Sie begutachten die Dokumentation der Änderung und lehnen sie entweder ab oder genehmigen sie. Meistens erkundigen sie sich nach weiteren Informationen oder Details, sodass es zu einem »Vorschlag-Ablehnung-Verbesserung-Wiedervorlage«-Kreislauf kommt, der so lange durchlaufen wird, bis alle zufrieden sind.

Ausfallplan

Und wenn die Änderung ein Reinfall ist? Das kommt öfter vor, als Sie vielleicht denken. Es muss einen *Ausfallplan* geben, der die erforderlichen Schritte festlegt, um zum Zustand der Infrastruktur vor der Änderung zurückzukehren. Zu einem solchen Plan gehört beispielsweise die Zurücknahme von Betriebssystemaktualisierungen, das Deinstallieren von Anwendungen oder die erneute Verwendung ausrangierter Geräte.

Julia von der Bayland Widgets Corporation möchte 16 Systeme im Entwicklungslabor upgraden. Das Management hat ihr das Upgrade von Windows 7 auf Windows 10 genehmigt und sie hat es der Reihe nach durchgeführt. Nach einigen Tagen beschweren sich mehrere Benutzer, dass eine wichtige CAD-Anwendung Probleme bereitet und gelegentlich abstürzt.

Julia sieht im Ausfallplan nach, in dem die erforderlichen Schritte dokumentiert sind, um das Upgrade rückgängig zu machen. Sie folgt diesen Schritten, macht sich dabei jeweils Notizen, und wartet nun auf weitere Anweisungen, wie sie die Computer im Entwicklungslabor upgraden kann, ohne dass es zu solchen Fehlschlägen kommt.

Änderungsdokumentation

Sämtliche Schritte einer Änderung müssen dokumentiert werden. Ein von einem CompTIA A+-Techniker geschnürtes Paket zur *Änderungsdokumentation* sollte nicht nur fast alle der genannten Schritte

umfassen, sondern auch Quittungen, Aufzeichnungen von Mehrarbeitszeit, eine Liste der geänderten Systeme, eine Liste neu angelegter Benutzer, unterzeichnete Formulare der Nutzungsbedingungen und so weiter.

28.3 Katastrophenvorbeugung und Wiederherstellung

Katastrophenvorbeugung und Wiederherstellung ist ein riesiges Themengebiet, das allen Netzwerktechnikern und Sicherheitsverantwortlichen sehr am Herzen liegt. Aus Sicht der CompTIA sind hier drei Punkte zu beachten: Gewährleistung der Stromversorgung, Sicherungs- und Wiederherstellungsverfahren sowie die Kontowiederherstellung.

28.3.1 Netzausfallsicherung

Computer benötigen eine geeignete und gleichmäßige Stromversorgung. Wie Sie aus Kapitel 7 wissen, stellen die Energieversorgungsunternehmen eine Wechselspannung bereit, die nicht immer ganz konstant ist. Es kann zu Spannungsabfällen, -einbrüchen und -spitzen kommen. Die Verwendung eines *Überspannungsschutzes*, der vor Spannungsspitzen schützt, und einer USV (unterbrechungsfreie Stromversorgung), die vor Spannungsabfällen und Stromausfällen schützt, kann den Unterschied zwischen einer ordnungsgemäß funktionierenden Computerkomponente und einem durchgeschmorten Briefbeschwerer bedeuten. Abbildung 28.5 zeigt eine typische USV.



Abb. 28.5: Unterbrechungsfreie Stromversorgung

Unternehmen sollten alle elektronischen Komponenten durch einen Überspannungsschutz oder eine USV schützen. Dazu gehören natürlich die PCs selbst, aber auch Switches, WAPs und Router. Jeder Server sollte über eine eigene USV verfügen, um die wertvollen Inhalte der Laufwerke zu schützen (siehe Abbildung 27.1 im vorigen Kapitel).

28.3.2 Sicherungs- und Wiederherstellungsverfahren

Techniker unterstützen die Benutzer und Unternehmen, indem sie Daten durch wohlbekannte und verlässliche Sicherungsverfahren schützen. Wenn etwas schiefgeht, werden Wiederherstellungsverfahren eingesetzt, damit den Anwendern schnellstmöglich wieder ein funktionierendes System zur Verfügung steht.

Backup-Optionen

In Kapitel 14 sind verschiedene Backup-Technologien und -Verfahren ausführlich beschrieben. Dieser Abschnitt konzentriert sich auf allgemeinere Fragestellungen: Welche Daten sollen gesichert werden

und wo? Und wie lange sollten ältere Backups aufbewahrt werden? Auf diese Fragen gibt es keine allgemeingültigen Antworten – sie hängen von sehr vielen Faktoren ab, etwa wie und mit welcher Art von Daten Sie arbeiten wie wichtig die Daten sind, welche Probleme genau aufgetreten sind, wie schnell Sie wieder arbeitsfähig sein müssen und wie viel Geld zur Lösung der Probleme bereitsteht.

Bei allen Verfahren muss ein Kompromiss zwischen dem Risiko eines Datenverlusts einerseits und der Bequemlichkeit, der Kosten und dem Aufwand andererseits eingegangen werden. Einige Punkte sind jedoch immer zu beachten:

- Viele Kopien sorgen dafür, dass Daten relativ sicher sind. Andererseits verursachen sie höhere Kosten und bergen das Risiko von Datenlecks.
- Investoren begrenzen Risiken durch Diversifizierung ihres Portfolios. Sie können das Risiko eines Datenverlusts begrenzen, indem Sie separate Sicherungen mit verschiedenen Backup-Programmen erstellen, die Sicherungskopien an verschiedenen Orten aufbewahren und sie auf unterschiedlicher Hardware speichern.
- Sicherungskopien außerhalb des Firmengebäudes aufzubewahren verringert das Risiko eines vollständigen Datenverlusts, erhöht aber auch die für eine Wiederherstellung erforderliche Zeit, wenn Sie nicht auch zusätzlich eine lokale Kopie aufbewahren.
- Die Einrichtung automatischer Backups ist etwas arbeitsaufwendiger, aber wenn das erledigt ist, sind sie manuellen Backups deutlich überlegen. Manuelle Backups sind zwar besser als nichts, aber Sie können sich darauf verlassen, dass die Benutzer vergessen, sie durchzuführen.

Die nächste Frage lautet, wie viele Daten Sie sichern möchten. Speicherplatz ist preiswert, aber die Kosten für das Speichern vieler Kopien häufiger Backups summieren sich schnell. Je nach Software oder Backup-Verfahren kommen viele verschiedene Strategien zum Einsatz, wie beispielsweise Komprimierung, Deduplizierung, inkrementelle Backups, die nur Änderungen seit dem letzten Backup sichern, und so weiter. Auf diese Weise soll die Menge der gespeicherten Daten verringert werden.

Häufig wird nur ein älteres Backup für einen bestimmten Zeitraum aufbewahrt. Man könnte beispielsweise für den letzten Tag stündliche Backups aufbewahren, für die vorhergehenden Tage der Woche aber nur jeweils eines, für den vorhergehenden Monat jeweils eines pro Woche, für das vorhergehende Jahr jeweils eines pro Monat, und für noch weiter zurückliegende Zeiträume nur eines pro Jahr. Bei inkrementellen Backups ist allerdings Vorsicht geboten: Die Wiederherstellung erfordert eine *lückenlose* Kette inkrementeller Backups seit dem letzten vollständigen Backup.

Hier ist ein Fallbeispiel für einen Techniker, der sich mit Backup-Optionen befasst. Chris ist bei Bayland Widgets für die Datensicherung der Buchhaltung verantwortlich, zu der fünf Arbeitsplatzrechner mit Windows 10 und ein Server mit wichtigen Buchhaltungsdaten gehören. Die Abteilung ist zwar nicht besonders groß, aber für den Unternehmensbetrieb *absolut unverzichtbar*. Chris darf sich also keinen Fehler erlauben. Betrachten wir also Backups auf Dateiebene, Backups wichtiger Anwendungen und Backups von Laufwerksabbildern.

Dateiebene

Ein Backup auf Dateiebene ist eine einfache Methode, die gewährleistet, dass wichtige Dateien gesichert werden. Dazu ist in der einfachsten Form keine spezielle Software erforderlich. Wählen Sie einfach eine Datei oder einen Ordner aus und kopieren Sie das Objekt auf ein externes Laufwerk, beispielsweise auf einen USB-Speicherstick (Abbildung 28.6) oder auf einen Cloud-basierten Speicher wie Dropbox. In diesem Fall würden alle Mitarbeiter der Buchhaltung ihre persönlichen Dateien an einem anderen Ort speichern. Chris müsste gewährleisten, dass alle Mitarbeiter Zugriff auf ein externes Laufwerk haben, oder aber Dropbox auf ihren Rechnern installieren und konfigurieren.

Manuelle Backups sind schön und gut, aber die bittere Wahrheit ist, dass Bayland Widgets eine Katastrophe oder einen ungewöhnlichen Zwischenfall wohl besser überstehen wird, wenn es ein Backup-Skript oder ein Programm gibt, das automatisch zu bestimmten Zeitpunkten (z.B. jede Nacht oder stündlich) läuft und alle wichtigen Daten sichert. In diesem Fall müsste Chris das entsprechende Skript oder Programm einrichten, so konfigurieren, dass die wichtigen Dateien gesichert werden, und überprüfen, ob das Backup wie geplant läuft.

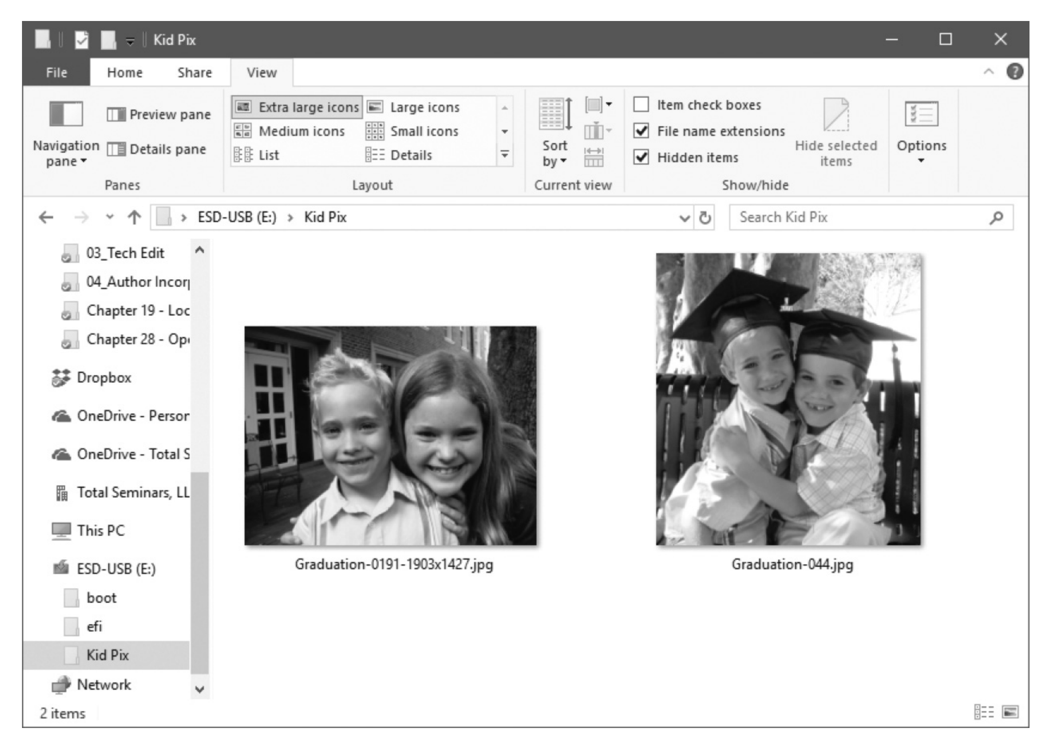


Abb. 28.6: Speichern der schönsten Familienfotos auf einem USB-Stick

Sowohl Windows als auch macOS bieten mit einem Dateiversionsverlauf bzw. Time Machine die Möglichkeit, lokale Backups auf Dateiebene zu erstellen, wie Sie aus Kapitel 14 wissen. Am besten funktioniert das mit einem per USB angeschlossenen Massenspeichergerät. Beide Verfahren sind besser als manuelle Backups und gut geeignet, versehentlich gelöschte oder überschriebene Dateien wiederherzustellen. Für eine Backup-Strategie zum Schutz betriebsnotwendiger Daten eines Unternehmens ist allerdings Backup-Software eines Drittanbieters und externer Speicherplatz erforderlich.

Wichtige Anwendungen

Wenn es um wichtige Anwendungen geht, sollten Sie zuerst das einfache Backup oder die Wiederherstellung ausprobieren. Zunächst einmal müssen Sie wissen, welche *Anwendungen* wirklich wichtig sind (für einen einzelnen Benutzer oder für das Unternehmen insgesamt). Darüber Buch zu führen, ist sicher keine schlechte Idee.

Zudem müssen Sie ermitteln, welche *Daten* unverzichtbar sind. Man kann leicht mehrere Tage damit zubringen, herauszufinden, wie eine Anwendung aufgebaut ist, was wo gespeichert wird und wie man wirklich alle Benutzereinstellungen sichern kann. Aber all das kann sich schon mit der nächsten Aktualisierung ändern. Je weniger Sie versuchen zu speichern, desto einfacher wird es, alles richtig zu machen und am Laufen zu halten.

So manche Software wird noch immer auf optischen Medien bereitgestellt, aber die meisten Anwendungen verlassen sich darauf, dass Downloads aus dem Internet zur Verfügung stehen. Deshalb ergibt es immer weniger Sinn, eine Sicherungskopie des Installationsprogramms einer Anwendung zu erstellen. Sie werden zweifelsohne die zusammen mit der Anwendung erzeugten Daten sichern und vielleicht gelingt es sogar, auch die Benutzereinstellungen zu sichern. Aber manchmal ist alles so sehr miteinander verwoben, dass eine Sicherungskopie des gesamten Programmpakets die einzige funktionierende Möglichkeit darstellt.

Bei der Wiederherstellung wichtiger Anwendungen müssen – minimal – die Schritte der Neuinstallation dokumentiert werden, sowie Folgendes:

- Lizenzschlüssel
- Wo das Installationsprogramm heruntergeladen werden kann (oder wo sich die Medien für eine Installation alter Schule finden lassen)
- Alle unverzichtbaren Installationsoptionen
- Informationen über ein Benutzerkonto oder Zugangsdaten, die für den Zugriff erforderlich sind

Diese Dokumentation unterstützt heutige und zukünftige Techniker, Hilfestellung zu leisten.

Wenn Sie eine installierte Anwendung wirklich mit einem Backup auf Dateiebene sichern wollen, müssen Sie den Speicherort der Programmdateien, der temporären Dateien, der Konfigurationsdateien und die Einstellungen in der Registry kennen. Das funktioniert nur – zumindest unter Windows – mithilfe von Programmen von Drittanbietern. Vielleicht finden Sie ein Programm eines Drittanbieters, das eine Sicherung aller erforderlichen Dateien verbreiteter Anwendungen ermöglicht. Ansonsten kommen Sie nicht darum herum, Ihre Backup-Software ausdrücklich so zu konfigurieren, dass sämtliche Daten gesichert werden.

Hinweis

Es gibt keine Garantie, dass die gesicherten Daten oder Einstellungen einer Version einer Anwendung mit einer anderen Version funktionieren. Sie können es probieren, aber seien Sie nicht überrascht, wenn Ihnen zahlreiche komplizierte Schritte abverlangt werden, um die Daten wiederherzustellen. So kann es beispielsweise erforderlich sein, *genau dieselbe Programmversion* zu installieren, mit der das Backup erstellt wurde, um die Daten wiederherzustellen. Anschließend müssen Sie die Anwendung erneut aktualisieren.

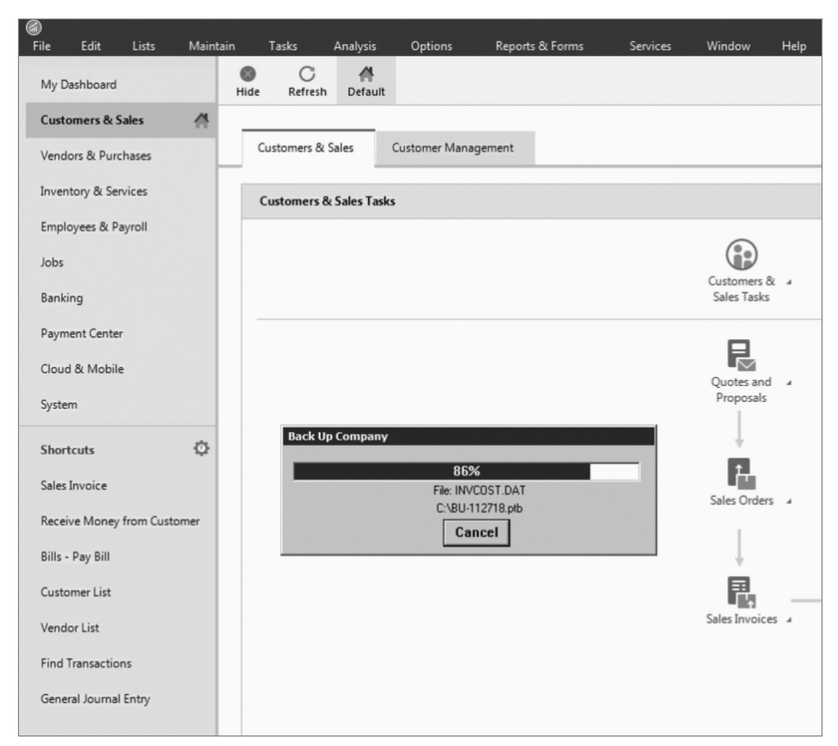


Abb. 28.7: Backup der Buchhaltungsdatenbank in Sage 50

Viele wichtige Anwendungen verfügen über eine integrierte Backup-Funktion. Die Buchhaltung verwendet beispielsweise die Software Sage 50, um die Finanzen der Bayland Widgets Corporation zu verwalten. Abbildung 28.7 zeigt die Backup-Option in Sage 50.

Das Entscheidende ist hier, dass einige dieser Anwendungen die Daten in der Cloud ablegen, andere hingegen, wie Sage 50 im obigen Beispiel, tatsächlich lediglich eine *lokale Kopie* der Anwendungsdaten exportieren. Chris muss hier gewährleisten, dass die Buchhaltungsmitarbeiter wissen, wie und wann sie Sage 50 verwenden, um ein Backup der Anwendungsdaten zu exportieren *und* dass die exportierten Anwendungsdaten auch wirklich Bestandteil des regelmäßig durchgeführten Backups sind.

Laufwerksabbilder

Bei einem Backup eines Laufwerksabbilds muss man sich nicht mit Dateien und Ordnern befassen, sondern sichert das gesamte Volume – inklusive des Betriebssystems, der Boot-Dateien, aller installierten Programme und sämtlicher Daten. Um zu entscheiden, wann ein Backup dieser Art geeignet ist, ist es hilfreich zu wissen, wie es funktioniert:

- Sie können ein Festplattenabbild auf einem leeren Laufwerk wiederherstellen, dieses in einen anderen Rechner einbauen und davon booten – sofern das System mit der neuen Hardware kompatibel ist. Auf diese Weise ist das System schnell wieder funktionsbereit.
- Laufwerksabbilder belegen viel Speicherplatz, oft mehrere Gigabyte. Sie enthalten die Daten des Betriebssystems und der Programme, die sich auf einem neu installierten System leicht wiederherstellen ließen.
- Da keine Auswahl getroffen werden muss, welche Dateien gesichert werden sollen, ist es für Techniker und Benutzer sehr einfach, sie zu erstellen.
- Man möchte nicht immer das gesamte Laufwerk wiederherstellen. Vielleicht enthält es Schadsoftware oder defekte Treiber. Oder Sie möchten den Benutzer auf ein neues Betriebssystem »umziehen«. Möglicherweise müssen auch nur ein paar beschädigte Dateien wiederhergestellt werden. In diesem Fall müssen Sie das gesamte Laufwerk mounten, sofern Ihre Backup-Software das unterstützt, und die Dateien heraussuchen, die der Benutzer benötigt.

Wenn Backups in Form von Laufwerksabbildern erstellt werden sollen, müsste Chris diese mit einem integrierten Tool planen (das Microsoft in Windows 10 allerdings für veraltet erklärt hat), oder ein Programm eines Drittanbieters benutzen (Abbildung 28.8).

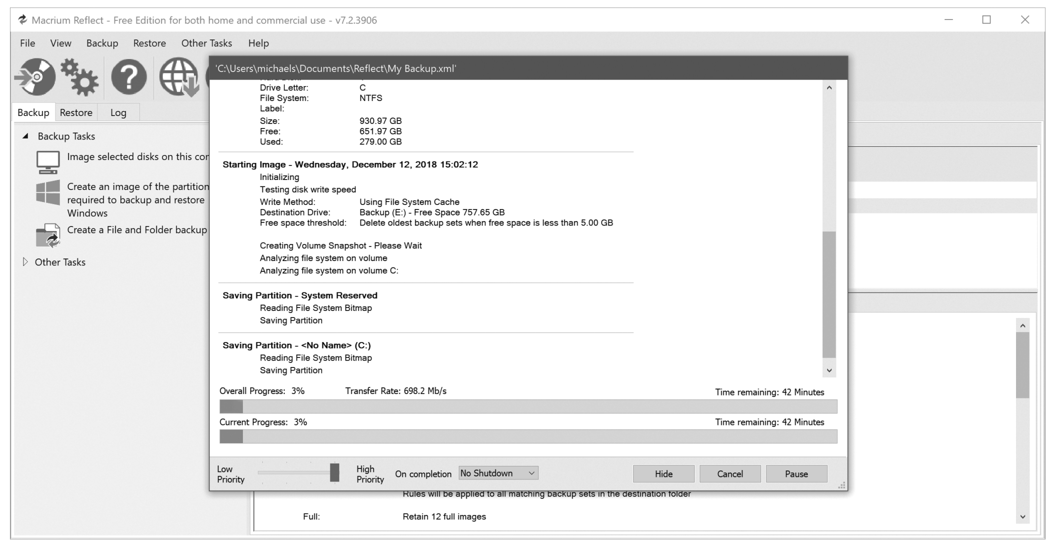


Abb. 28.8: Macrium Reflect – kostenlose Version

Wenn die Software inkrementelle Backups gestattet, muss angegeben werden, wie oft diese erstellt und wann vollständige Backups durchgeführt werden sollen. Bedenken Sie jedoch, dass für die Wiederherstellung eine lückenlose Kette inkrementeller Backups seit dem letzten vollständigen Backup erforderlich ist!

Cloud-Speicher und lokaler Speicher

Backups auf Servern im Internet (Cloud-Speicher) verdrängen zunehmend lokale Backups. Dieser Trend bringt eine Reihe von Problemen mit sich. Betrachten wir also die guten Seiten des Cloud-Speichers und stellen ihnen die Vorteile des lokalen Speichers gegenüber.

Zunächst einmal sind Cloud-Backups überall verfügbar. Man benötigt natürlich eine Internetverbindung, aber für Backups von Dateien ist das eine hervorragende Option. Beispielsweise verfügen iPhone-Benutzer über Benutzerkonten bei Apples iCloud und können automatisch Backups von ihren Fotos und Videos erstellen. Ein einfaches Benutzerkonto ist kostenlos, für zusätzlichen Speicherplatz ist eine monatliche oder jährliche Gebühr zu entrichten. Der Cloud-Speicher bietet Schutz vor Datenverlust, wenn Geräte verloren gehen oder beschädigt werden. Ihre Daten sind sicher. (Für Android gibt es natürlich vergleichbare Angebote.)

Nachteilig ist, dass größere Backups (wie das Erstellen eines Laufwerksabbilds) beim Cloud-Speicher langwierig sind. Selbst bei heutigen Upload-Datenraten von mehr als 10 Mbps nimmt der Upload eines vollständigen Laufwerksabbilds viel Zeit in Anspruch. Beispielsweise würde der Upload eines 1 TB großen Abbilds bei einer kontinuierlichen Datenrate von 10 Mbps länger als einen Tag dauern.

Bei der Fotosammlung Ihrer Eltern ist das keine große Sache, das sieht aber anders aus, wenn Sie wirklich gigantische Datenmengen mit der Cloud austauschen wollen und AWS dafür bezahlen, bis unter die Decke mit Festplatten vollgestopfte Container mit einer Speicherkapazität von mehr als *100.000 Terabyte* per Sattelzug zu transportieren. Bei Bedarf steht sogar ein Begleitschutz zur Verfügung.

Bei lokalem Speicher ist es umgekehrt. Zum einen benötigt man keine Internetverbindung (und keinen Parkplatz für den Sattelzug), sondern nur lokale Speichermedien. Massenspeichergeräte sind preiswert und einfach zu implementieren, deshalb ist lokaler Speicher für Backups von Dateien und Laufwerksabbilder gut geeignet.

Der Nachteil von lokalem Speicher ist, dass er überhaupt keinen Schutz vor *lokalen* Katastrophen bietet. Ich wohne in Houston, Texas, und hier gibt es mehr oder weniger regelmäßig Hurrikans. Bislang ist meine Firma noch keinem dieser Wirbelstürme zum Opfer gefallen, aber von Mai bis November besteht diese Gefahr jedes Jahr. Wenn wir unser geistiges Eigentum nur durch lokale Backups schützen würden, liefen wir jedes Jahr Gefahr, alles zu verlieren.

Deshalb verwenden wir konsequenterweise beide Sicherungsverfahren. Das ist zwar etwas komplizierter, aber die Nutzung von Cloud-Speicher für unverzichtbare Daten und lokalem Speicher für typische tägliche Backups bedeutet, dass unsere Daten sicher sind – und das ist eine feine Sache!

Überprüfung des Backups

Rechnen Sie in der CompTIA A+-Zertifizierungsprüfung 1002 mit Fragen zum Thema *Überprüfung des Backups*. Die Regel lautet: *Sie müssen Ihr Backup immer überprüfen.* Es ist durchaus möglich, dass man Unmengen an Zeit und Geld in tägliche Backups und die Befolgung aller Richtlinien investiert, wie etwa verschlüsselte Kopien an mehreren verschiedenen Orten aufzubewahren und in der Cloud zu speichern, nur um beim Eintreten einer Katastrophe feststellen zu müssen, dass sich die Dateien und Laufwerksabbilder nicht erfolgreich wiederherstellen lassen. Backup-Strategien, die keine Überprüfung des Backups vorsehen, sind nicht mehr als schöner Schein. Genauso gut könnten Sie eine defekte Festplatte unter das Kopfkissen legen und hoffen, dass sich die Zahnfee darum kümmert.

Leider ist die Überprüfung des Backups gar nicht so einfach, wie man denkt. Sie müssen in der Lage sein, die gesicherten Daten, seien es nun Dateien oder Laufwerksabbilder, exakt so wiederherzustellen, dass sie dem vorherigen Zustand entsprechen. So weit, so gut, aber tatsächlich ist es etwas verzwickter. Nehmen wir an, Sie vergleichen unmittelbar nach dem Erstellen eines Backups die gesicherten Dateien mit denen auf dem Laufwerk, um zu gewährleisten, dass sie identisch sind. Aber

wenn die Dateien auf dem Laufwerk beschädigt sind, dann garantiert die Überprüfung lediglich, dass Sie die defekten Dateien akribisch kopiert haben.

Backup-Werkzeuge, die Ihre Zeit und Ihr Geld wert sind, bieten zwar die Möglichkeit, zu überprüfen, dass sich ein Backup nicht geändert hat, seit es gespeichert wurde, das ist jedoch kein Ersatz dafür, regelmäßig zu testen, ob sich wichtige Laufwerksabbilder, Anwendungen und Daten nicht nur wiederherstellen lassen, sondern auch *tatsächlich nutzbar* sind.

In der Praxis bedeutet das: Wenn Ihre Software Backups überprüfen kann, sollten Sie das nutzen. Es spielt jedoch keine Rolle, was Ihre Backup-Software leistet, die Backups müssen regelmäßig getestet werden. Vollständige Laufwerksabbilder sollten sich wiederherstellen lasen und booten, und alle wichtigen Anwendungen sollten funktionieren. Es ist schwierig, alles zu überprüfen, aber wichtige Dateien sollten sich nach dem Wiederherstellen mit der entsprechenden Anwendung öffnen lassen. Und wichtige Anwendungen sollten sorgfältig getestet werden, um zu gewährleisten, dass unverzichtbare Einstellungen, Konfigurationen und Daten funktionieren bzw. lesbar sind.

28.3.3 Kontowiederherstellung

Was tun Sie, wenn Sie einen Benutzernamen oder ein Kennwort vergessen haben? Die *Kontowiederherstellung* bietet die Möglichkeit, Zugriff auf Ihr altes Kennwort zu erlangen oder dem Benutzerkonto ein temporäres Kennwort zuzuweisen. Der Benutzer wird dann bei der ersten Anmeldung aufgefordert, ein dauerhaftes Kennwort einzurichten.

In einer Domänenumgebung kümmert sich der Domänenadministrator um die Wiederherstellung von Kennwörtern oder Benutzerkonten. Techniker und Benutzer müssen ihn lediglich kontaktieren.

In einer lokalen Umgebung oder einer Arbeitsgruppe, muss ein Techniker schon eher tätig werden. Sie können Programme von Drittanbietern verwenden, um Kennwörter zu löschen und es dem Benutzer zu ermöglichen, sich anzumelden und ein neues Kennwort einzurichten.

Anstatt zu versuchen, vergessene Kennwörter wiederherzustellen, sollten Sie schon vorher Vorsichtsmaßnahmen treffen und eine Kennwortrücksetzdiskette erstellen. In Windows 10 gibt es unter SYSTEMSTEUERUNG|BENUTZERKONTEN die Option KENNWORTRÜCKSETZDISKETTE ERSTELLEN. Oder geben Sie in das Suchfeld in der Taskleiste »Kennwortrücksetz...« ein, um diese Option anzuzeigen (Abbildung 28.9). Beachten Sie jedoch, dass dies nur mit lokalen Benutzerkonten funktioniert. Wenn Sie mit einem Microsoft-Konto angemeldet sind, ist es nicht möglich, eine Kennwortrücksetzdiskette zu erstellen. Notieren Sie in diesem Fall Ihren Benutzernamen und Ihr Kennwort auf einem kleinen Kärtchen und bewahren Sie diese in einem Safe auf. Sie dürfen mir glauben: Sie wollen diese Zugangsdaten wirklich nicht verlieren.

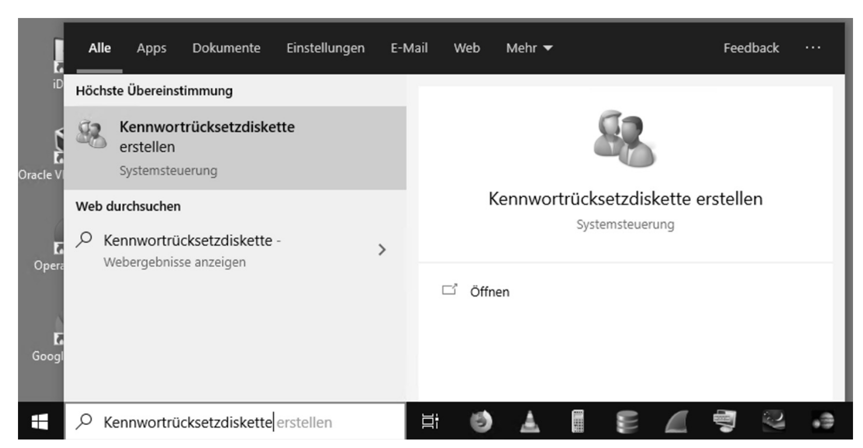


Abb. 28.9: Kennwortrücksetzdiskette für ein lokales Benutzerkonto erstellen

Jenseits von A+

Puh! Sie haben gerade die Lektüre eines Buchs mit über 1300 Seiten abgeschlossen, das alles behandelt, was Sie für das Bestehen der CompTIA A+-Zertifizierungsprüfungen 1001 und 1002 wissen müssen. Glückwunsch! Und was kommt als Nächstes?

Zum einen sollten Sie sich noch einmal die Einleitung ansehen. Nutzen Sie die Beispiele für Prüfungsfragen und suchen Sie online nach weiteren Quellen, um noch mehr über die Art der Prüfungsfragen, die auf Sie zukommen, in Erfahrung zu bringen.

Zum anderen sollten Sie einen Prüfungstermin vereinbaren, falls Sie das noch nicht getan haben (Diamanten und Druck und so). Wenn ein Ende in Sicht ist, kann man sich besser auf die Aufgabe konzentrieren.

Und wenn Sie beide Prüfungen bestanden haben, stellt sich wieder die eingangs gestellte Frage: Was kommt als Nächstes? Der folgerichtige nächste Schritt ist die Vorbereitung auf die Prüfungen CompTIA Network+ und CompTIA Security+. Damit vollenden Sie die Core-Zertifizierungen der CompTIA und sind für die heutige hochgradig vernetzte und durch Sicherheitsrisiken bedrohte Welt gewappnet. Es gibt viele tolle Autoren und Macher von Lernvideos, die ausgezeichnetes Material zu den Themengebieten Network+ und Security+ anbieten (zu denen ich mich auch zähle), es ist also gar nicht schwer, Lehrmaterial zu finden.

Viel Glück dabei – und bleiben Sie in Kontakt!



28.4 Wiederholung

28.4.1 Fragen

1. Arthur aus der Buchhaltung ruft Henry an und berichtet, dass seine Tastatur nicht funktioniert. Das scheint ein bekanntes Problem zu sein, das ein anderer Techniker erst kürzlich erwähnt hat. Wo könnte Henry Informationen über dieses Problem finden?

   A. Änderungsdokumentation

   B. Zwischenfallberichte

   C. Dokumentation des Änderungsmanagements

   D. Dokumentation des Risikomanagements

2. Annie möchte mehrere Mac-Laptops, die den Vertriebsmitarbeitern bereitgestellt werden, kennzeichnen, damit sie am Eingang einen Scanner einrichten kann, der registriert, wenn jemand mit einem Laptop das Büro betritt oder verlässt. Wie kann sie das erreichen?

   A. Mit einem Barcode-Aufkleber.

   B. Mit einem RFID-Etikett.

   C. Sie muss dem Änderungsausschuss einen entsprechenden Antrag vorlegen.

   D. Das funktioniert nicht, weil auf den Rechnern macOS läuft.

3. Johanna hat beantragt, die Tintenstrahldrucker in der Marketing-Abteilung durch Farblaserdrucker zu ersetzen. Zweck der Änderung ist die Senkung der Kosten pro Druckseite, denn Toner ist preiswerter als Tinte und die Laserdrucker haben eine höhere Lebenserwartung als die Tintenstrahldrucker. Derzeit sind in der Marketing-Abteilung drei Tintenstrahldrucker in Betrieb. Was ist der nächste folgerichtige Schritt?
   A. Sie sollte in ihrem Antrag ergänzen, wie viel die neuen Drucker kosten.
   B. Sie sollte eine Risikoanalyse durchführen, um mögliche negative Folgen zu ermitteln.
   C. Sie sollte die Dokumentation für die neuen Drucker herunterladen und eine Anwenderschulung für ihre Nutzung vorbereiten.
   D. Sie sollte sich mit ihrem ursprünglichen Vorschlag an den Änderungsausschuss wenden.
4. Der Änderungsausschuss hat Johannes Antrag geprüft und genehmigt. Was ist der nächste Schritt?
   A. Einen Ausfallplan erstellen, für den Fall, dass die Qualität der Ausdrucke den Anforderungen der Marketing-Abteilung nicht genügt.
   B. Den Ausfallplan testen.
   C. Die Änderungsdokumentation fertigstellen.
   D. Den Änderungsplan umsetzen.
5. Welcher allgemeine Begriff beschreibt das Erstellen eines Plans für heutige und zukünftige Techniker, die das Netzwerk ändern oder reparieren müssen?
   A. Änderungsdokumentation
   B. Änderungsmanagementprozess
   C. Managementdokumentation
   D. Netzwerkdokumentation
6. Welcher allgemeine Begriff beschreibt die Möglichkeit, dass Unternehmen Änderungen an der IT-Infrastruktur auf sichere und kostengünstige Weise vornehmen?
   A. Änderungsdokumentation
   B. Änderungsmanagementprozess
   C. Managementdokumentation
   D. Netzwerkdokumentation
7. Als Teil des Änderungsmanagementprozesses ist die Anwenderschulung ein wichtiger Bestandteil wovon?
   A. Ausfallplan
   B. Zugänglichkeitsschulung
   C. Benutzerakzeptanz
   D. Risikoanalyse
8. Welches Gerät schützt Computer vor Spannungseinbrüchen und Stromausfällen?
   A. GPS
   B. Überspannungsschutz
   C. Überspannungsunterdrückung
   D. USV
9. Wie kann Emilia aus der Vertriebsabteilung ihren Ordner mit Kundeninformationen vor Naturkatastrophen schützen?
   A. Lokales Backup auf Dateiebene
   B. Cloud-basiertes Backup auf Dateiebene
   C. Lokales Backup eines Laufwerkabbilds
   D. Cloud-basiertes Backup eines Laufwerkabbilds

10. Wozu dient eine Kennwortrücksetzdiskette in Windows 10?
    A. Sie ermöglicht eine Anmeldung ohne Angabe eines Kennworts.
    B. Sie ermöglicht es, ein Kennwort mit einem entfernten Benutzer zu teilen.
    C. Sie ermöglicht eine Kontowiederherstellung, wenn man das Kennwort vergessen hat.
    D. Sie ermöglicht ein veränderliches Kennwort zwecks Erhöhung der Sicherheit.

28.4.2 Antworten

1. **B.** Henry sollte in den Zwischenfallberichten nachsehen, ob es mit dem Computer an diesem Arbeitsplatz schon früher Probleme gab.
2. **B.** Annie sollte RFID-Etiketten zur Kennzeichnung der Laptops verwenden und am Eingang einen RFID-Scanner einrichten, um zu registrieren, wenn jemand mit einem Laptop das Gebäude betritt oder verlässt.
3. **A.** Johanna sollte in ihrem Antrag angeben, wie teuer die neuen Drucker sind.
4. **A.** Wenn der Änderungsausschuss die Änderung genehmigt hat, sollte Johanna gewährleisten, dass es einen Ausfallplan gibt, falls es irgendwelche unvorhergesehenen oder negativen Folgen gibt.
5. **D.** Das Erstellen eines Plans für heutige und zukünftige Techniker, die das Netzwerk ändern oder reparieren müssen, wird durch den Begriff *Netzwerkdokumentation* beschrieben.
6. **B.** Die Möglichkeit, dass Unternehmen Änderungen an der IT-Infrastruktur auf sichere und kostengünstige Weise vornehmen, wird durch den Begriff *Änderungsmanagementprozess* beschrieben.
7. **C.** Die Anwenderschulung ist für die Benutzerakzeptanz von großer Bedeutung.
8. **D.** Eine unterbrechungsfreie Stromversorgung (USV) schützt Computer vor Spannungseinbrüchen und Stromausfällen.
9. **B.** Emilia sollte ein Cloud-basiertes Backup auf Dateiebene verwenden, um ihren Ordner mit Kundeninformationen vor Naturkatastrophen schützen.
10. **C.** Eine Kennwortrücksetzdiskette ermöglicht eine Kontowiederherstellung, wenn man das Kennwort vergessen hat.

Zuordnung zu den Zielen von CompTIA A+



A.1 Zielzuordnung für CompTIA A+ 220-1001

Thema	Kapitel
1.0 Mobile Geräte	
1.1 Installation und Konfiguration von Laptop-Hardware und Komponenten	
Austauschbare Komponenten	23
Tastatur	23
Festplatte	23
SSD, Hybrid, magnetische Festplatten	23
1,8- und 2,5-Zoll-Laufwerke	23
Arbeitsspeicher	23
Smartcard-Lesegeräte	23
Optische Laufwerke	23
WLAN-/Bluetooth-Karte	23
Mobilfunkkarte	23
Grafikkarte	23
Mini-PCIe	23
Bildschirm	23
Stromanschluss	23
Akku	23
Touchpad	23
Kunststoffbauteile und -rahmen	23
Lautsprecher	23
Mainboard	23
CPU	23
1.2 Installation der Komponenten eines Laptop-Bildschirms	
Typen	23
LCD	23
OLED	23
WLAN-Antennenanschluss/Antennenposition	23
Webcam	23
Mikrofon	23

Thema	Kapitel
Inverter	23
Digitizer/Touchscreen	23
1.3 Funktionen von Laptops	
Spezielle Funktionstasten und Schalter	23
Externe Bildschirme	23
WLAN aktivieren/deaktivieren	23
Mobilfunk aktivieren/deaktivieren	23
Lautstärkeeinstellung	23
Bildschirmhelligkeit	23
Bluetooth aktivieren/deaktivieren	23
Touchpad aktivieren/deaktivieren	23
Bildschirmausrichtung	23
Medientasten (Wiedergabe, Vor- und Zurückspulen)	23
GPS aktivieren/deaktivieren	23
Flugmodus	23
Dockingstation	23
Port-Replikator	23
Laptop-Schlösser und Sicherungskabel	23
Umklappbare/abnehmbare Bildschirme	23
1.4 Eigenschaften weiterer mobiler Geräte	
Tablets	24
Smartphones	24
Wearables	24
Smartwatches	24
Fitness-Armbänder	24
VR/AR-Headsets	24
E-Book-Lesegeräte	24
GPS	24
1.5 Konfiguration von Anschlüssen und Zubehör weiterer mobiler Geräte	
Verbindungsmöglichkeiten	
Kabelgebunden	24
Micro-USB, Mini-USB, USB-C	24
Lightning	24
Tethering	24
Herstellerspezifische Anschlüsse (Daten/Strom)	24
Drahtlos	24
NFC	24

Thema	Kapitel
Bluetooth	24
Infrarot	24
Hotspot	24
Zubehör	24
Headsets	24
Lautsprecher	24
Gamepads	24
Akkus/Powerbanks	24
Schutzhüllen und wasserdichte Gehäuse	24
Kreditkartenleser	24
Speicherkarten	24
1.6 Konfiguration von Netzwerkverbindungen und Apps auf mobilen Geräten	
Drahtlose/Mobilfunk-Netzwerke (aktivieren/deaktivieren)	24
Hotspot	24
Tethering	24
Flugmodus	24
Bluetooth	24
Bluetooth aktivieren	24
Kopplung von Bluetooth-Geräten	24
Nach Bluetooth-Geräten suchen	24
Eingabe des PIN-Codes	24
Verbindung testen	24
Konfiguration von E-Mail	24
POP3	24
IMAP	24
Port- und SSL-Einstellungen	24
S/MIME	24
Integrierte E-Mail-Konfiguration durch kommerzielle Anbieter	24
iCloud	24
Google/Inbox	24
Exchange Online	24
Yahoo	24
PRL-, PRI- und Baseband-Updates	24
Firmware für Funkverbindungen	24
IMEI und IMSI	24
VPN	24

Thema	Kapitel
1.7 Synchronisierung von mobilen Geräten	
Synchronisierungsverfahren	24
Synchronisierung mit der Cloud	24
Synchronisierung mit dem Desktop	24
Synchronisierung im Auto	24
Typen der zu synchronisierenden Daten	24
Kontakte	24
Anwendungen	24
E-Mail	24
Bilder und Fotos	24
Videos	24
Kalender	24
Lesezeichen	24
Dokumente	24
Positionsdaten	24
Daten sozialer Medien	24
E-Books	24
Kennwörter	24
Single-Sign-On	24
Synchronisierungssoftware für den PC	24
Verbindungstypen bei der Synchronisierung	24
2.0 Netzwerke	
2.1 TCP- und UDP-Ports, Protokolle und deren Aufgaben	
Ports und Protokolle	21
21 – FTP	21
22 – SSH	21
23 – Telnet	21
25 – SMTP	21
53 – DNS	21
80 – HTTP	21
110 – POP3	21
143 – IMAP	21
443 – HTTPS	21
3389 – RDP	21
137 – 139 – NetBIOS/NetBT	21
445 – SMB/CIFS	21
427 – SLP	21

Thema	Kapitel
548 – AFP	21
67/68 – DHCP	21
389 – LDAP	21
161/162 – SNMP	21
TCP vs. UDP	19
2.2 Vergleich und Gegenüberstellung von Netzwerkgeräten sowie deren Funktionen und Eigenschaften	
Router	18, 19
Switches	18, 19
Mit Management-Funktionen	19
Ohne Management-Funktionen	19
Access Points	20
Cloud-basierter Netzwerk-Controller	20
Firewall	27
Netzwerkkarte	18
Repeater	18
Hub	18
Kabelmodem/DSL-Modem	21
Bridge	18
Patchfeld	18
Power over Ethernet (PoE)	20
Switch	20
Ethernet over Power	18
2.3 Installieren und Konfigurieren eines SOHO-Netzwerks (Small Office, Home Office)	
Funktionalität von Router und Switch	18, 19
Einstellungen von Zugriffspunkten	20
IP-Adressierung	19
Konfiguration von Netzwerkkarten	
kabelgebundene	18, 19
drahtlose	20
Konfiguration von Endbenutzergeräten	25
Konfiguration von IoT-Geräten	21
Thermostat	21
Lichtschalter	21
Überwachungskameras	21
Türschlösser	21
Sprachgesteuerte Lautsprecher/digitaler Assistent	21

Thema	Kapitel
Konfiguration von Kabelmodem/DSL-Modem	21
Einstellungen der Firewall	27
DMZ	27
Portweiterleitung	27
NAT	21, 27
UPnP	21
Zugang gewähren/verweigern	27
MAC-Adressfilterung	27
QoS	21
WLAN-Konfiguration	
Verschlüsselung	20, 27
Kanäle	20
QoS	21
2.4 Vergleich und Gegenüberstellung drahtloser Netzwerkstandards	
802.11a	20
802.11b	20
802.11g	20
802.11n	20
802.11ac	20
Frequenzbereiche	20
2,4 GHz	20
5 GHz	20
Kanäle	20
1 bis 11	20
Bluetooth	20
NFC	24
RFID	28
Zigbee	21
Z-Wave	21
3G	21
4G	21
5G	21
LTE	21
2.5 Eigenschaften und Zweck von Netzwerkdiensten	
Servertypen	
Webserver	18, 21
Dateiserver	18

Thema	Kapitel
Druckserver	18, 26
DHCP-Server	19
DNS-Server	19
Proxyserver	21
Mailserver	18, 24
Authentifizierungsserver	19
syslog	16
Internet-Appliance	
UTM	27
IDS	27
IPS	27
VPN-Endpunkte	21
Ältere Systeme	18
2.6 Netzwerkkonfiguration	
IP-Adressierung	19
statische	19
dynamische	19
APIPA	19
Linklokal	19
DNS	19
DHCP	19
Reservierungen	19
IPv4 und IPv6	19
Subnetzmaske	19
Gateway	19
VPN	21, 24
VLAN	19
NAT	21
2.7 Vergleich und Gegenüberstellung von Netzwerkverbindungen und deren Eigenschaften	
Internetverbindungsarten	21
Kabelanschluss	21
DSL	21
Telefoneinwahl	21
Glasfaser	21
Satellit	21
ISDN	21

Thema	Kapitel
Mobilfunk	21
Tethering	21
Mobiler Hotspot	21
Internetverbindung per Richtfunkstrecke	21
Netzwerktypen	
LAN	18
WAN	18
PAN	20
MAN	21
WMN	20
2.8 Einsatz der einer konkreten Situation angemessenen Werkzeuge	
Crimpzange	18
Abisolierzange	18
Multimeter	7
Tonsonden	19
Kabeltester	18, 19
Loopback-Stecker	19
Punchdown-Tool	18
WLAN-Analyzer	20
3.0 Hardware	
3.1 Kabel und Stecker und deren Zweck	
Netzwerkkabel	18
Ethernet	18
Cat5	18
Cat5e	18
Cat6	18
Plenum	18
Shielded Twisted-Pair	18
Unshielded Twisted-Pair	18
568A/B	18
Glasfaser	18
Koaxialkabel	18
Geschwindigkeit und Begrenzung der Kabellänge	18
Videokabel	17
VGA	17
HDMI	17
Mini-HDMI	17

Thema	Kapitel
DisplayPort	17
DVI	17
DVI-DDVI-I	17
Mehrzweckkabel	
Lightning	24
Thunderbolt	10
USB	10
USB-C	10, 24
USB 2.0	10
USB 3.0	10
Peripheriekabel	10
Seriell	10
Festplattenkabel	8
SATA	8
IDE	8
SCSI	8
Adapter	
DVI auf HDMI	17
USB auf Ethernet	23
DVI auf VGA	17
3.2 Gebräuchliche Anschlüsse	
RJ-11	18
RJ-45	18
RS-232	10
BNC	18
RG-59	18
RG-6	18
USB	10
Micro-USB	10
Mini-USB	10
USB-C	10, 24
DB-9	10
Lightning	24
SCSI	8
eSATA	8
Molex	7, 8

Thema	Kapitel
3.3 RAM-Typen und deren Charakteristika	
RAM-Typen	4
SODIMM	4
DDR2	4
DDR3	4
DDR4	4
Single-Channel	4
Dual-Channel	4
Triple-Channel	4
Fehlerkorrektur	4
Parität vs. Nicht-Parität	4
3.4 Auswahl, Installation und Konfiguration von Speichergeräten	
Optische Laufwerke	10
CD-ROM/CD-RW	10
DVD-ROM/DVD-RW/DVD-RW DL	10
Blu-ray	10
BD-R	10
BD-RE	10
SSDs	8
M.2-Laufwerke	8
NVMe	8
SATA 2.5	8
Magnetische Festplatten	8
5400 U/min	8
7200 U/min	8
10000 U/min	8
15000 U/min	8
Größen	8
2,5 Zoll	8
3,5 Zoll	8
Hybrid-Laufwerke	8
Flash-Speicher	10
SD-Karte	10
CompactFlash	10
Micro-SD-Karte	10
Mini-SD-Karte	10
xD	10

Thema	Kapitel
Konfigurationen	8
RAID 0, 1, 5, 10	8
Hot-swappable	8
3.5 Installation und Konfiguration von Mainboards, CPUs und Erweiterungskarten	
Formfaktoren	6
ATX	6
mATX	6
ITX	6
mITX	6
Erweiterungssteckplätze	6
PCI	6
PCIe	6
Riser-Karte	6
Sockeltypen	3
SATA	8
IDE	8
Anschlüsse an der Vorderseite	6
Interne USB-Anschlüsse	6
BIOS/UEFI-Einstellungen	5
Boot-Optionen	5
Firmware-Updates	5
Sicherheitseinstellungen	5
Schnittstellenkonfiguration	5
Sicherheit	5
Kennwörter	5
Laufwerksverschlüsselung	5
TPM	5
LoJack	5
Secure Boot	5
CMOS-Batterie	5
CPU-Merkmale	3
Einkernprozessor	3
Mehrkernprozessor	3
Virtualisierungstechnologie	3
Hyperthreading	3
Geschwindigkeiten	3
Übertaktung	3

Thema	Kapitel
Kompatibilität	3
AMD	3
Intel	3
Kühlung	3
Lüfter	3
Kühlkörper	3
Flüssigkeitskühlung	3
Wärmeleitpaste	3
Erweiterungskarten	
Grafikkarten	6, 17
Onboard	6, 17
eigenständige	6, 17
Soundkarte	6, 10
Netzwerkkarte	6, 18–21
USB-Erweiterungskarte	6, 10
eSATA-Karte	6, 8
3.6 Zweck und Verwendung verschiedener Peripheriegeräte	
Drucker	26
Flachbettscanner	26
Barcode- und QR-Scanner	10
Monitore	17
VR-Headsets	17, 24
Optische Laufwerke	10
DVD-Laufwerk	10
Maus	10
Tastatur	10
Touchpad	10, 23
Unterschriftendigitalisierung	10
Gamepads	10
Kamera/Webcam	10
Mikrofon	10
Lautsprecher	10
Headset	10, 24
Projektor/Beamer	17
Lumen/Helligkeit	17
Externe Speicherlaufwerke	8
KVM	10

Thema	Kapitel
Magnetkartenleser/Chipkartenleser	24
NFC/Zahlungssystem	24
Smartcard-Lesegerät	10
3.7 Netzteiltypen und deren Merkmale	
Eingangsspannung 110 bzw. 220 Volt	7
Ausgangsspannung 5,5 und 12 Volt	7
24-Pin-Mainboard-Adapter	7
Wattleistung	7
Anzahl und Art der mit Spannung versorgten Geräte	7
3.8 Auswahl und Konfiguration der angemessenen Komponenten für einen maßgeschneiderten PC, der den Anforderungen des Kunden entspricht	
CAD/CAM- oder Grafik-Arbeitsplatzrechner	11
Mehrkernprozessor	11
Hochwertige Grafikkarte	11
Maximale RAM-Ausstattung	11
Multimedia-Arbeitsplatzrechner	11
Spezielle Sound- und Grafikkarten	11
Große, schnelle Festplatten	11
Mehrere Bildschirme	11
Virtualisierte Arbeitsplatzrechner	11
Maximale RAM-Ausstattung und Mehrkernprozessoren	11
Spiele-PC	11
Mehrkernprozessor	11
Hochwertige Grafikkarte/Grafikprozessor	11
Hochwertige Soundkarte	1
Hochwertige Kühlung	11
Thick-Client	11
Desktop-Anwendungen	11
Erfüllung der empfohlenen Systemanforderungen	11
Thin-Client	11
Grundlegende Anwendungen	11
Erfüllung der minimalen Systemanforderungen	11
Netzwerkverbindung	1
NAS-Geräte	11
Medienstreaming	11
File Sharing	11
Gigabit-Netzwerkkarte	11
RAID-Verbund	11

Thema	Kapitel
3.9 Installation und Konfiguration gängiger Geräte	
Desktop	
Thin-Client	11
Thick-Client	11
Benutzerkonto einrichten und konfigurieren	11
Laptop/Smartphone/Tablet	
Touchpad konfigurieren	23
Touchscreen konfigurieren	24
Anwendungen installieren und konfigurieren	24
Synchronisierung konfigurieren	24
Benutzerkonto einrichten und konfigurieren	24
WLAN-Einstellungen	24
3.10 Installation und Konfiguration von Druckern und SOHO-Multifunktionsgeräten	
Treiber für das Betriebssystem verwenden	26
Einstellungen	26
Beidseitiger Druck	26
Sortierung	26
Ausrichtung	26
Druckqualität	26
Gemeinsame Nutzung	26
Kabelgebunden	26
USB	26
Seriell	26
Ethernet	26
Drahtlos	26
Bluetooth	26
802.11 (a, b, g, n, ac)	26
Infrastruktur- und Ad-hoc-Modus	26
Integrierter Druckserver	26
Drucken über die Cloud	26
Öffentlich zugängliche/gemeinsam genutzte Geräte	26
Netzwerkfreigabe lokaler Drucker	26
TCP/Bonjour/AirPrint	26
Datenschutz	26
Benutzerauthentifizierung am Gerät	26
Festplatten-Caching	26

Thema	Kapitel
3.11 Installation und Wartung von Druckern	
Laserdrucker	26
Belichtungstrommel, Fixiereinheit, Papiertransport, Papiereinzug, Trennelemente, Duplexeinheit	26
Druckvorgang: verarbeiten, laden, belichten, entwickeln, übertragen, fixieren, reinigen	26
Wartung: Toner ersetzen, Wartungskit verwenden, Kalibrierung, Reinigen	26
Tintenstrahldrucker	26
Tintenpatronen, Druckkopf, Rollen, Duplexeinheit, Transportmechanismus	26
Kalibrierung	26
Wartung: Druckkopf reinigen, Tintenpatronen ersetzen, Papierstau beseitigen	26
Thermodrucker	26
Papiereinzug, Heizelement des Thermodruckkopfs	26
Spezialpapier für Thermodruck	26
Wartung: Papier nachlegen, Heizelement reinigen, Abrieb entfernen	26
Anschlagdrucker	26
Druckkopf, Farbband, Traktortransport Papierdurchschläge/Kohlepapier	26
Wartung: Farbband und Druckkopf ersetzen, Papier nachfüllen	26
Virtuelle Drucker	26
Ausgabe als PDF, XPS oder als Bild	26
3-D-Drucker	26
Kunststoff-Filamente	26
4.0 Virtualisierung und Cloud-Computing	
4.1 Vergleich und Gegenüberstellung von Konzepten des Cloud-Computings	
Gängige Modelle	22
IaaS	22
SaaS	22
PaaS	22
Public Cloud, Private Cloud, Hybrid Cloud und Community Cloud	22
Gemeinsam genutzte Ressourcen	22
Intern vs. extern	22
Rapid Elasticity	22
On-demand (bei Bedarf)	22
Ressourcenbündelung	22
Kostenpflichtige Dienste entsprechend der Nutzung	22
Externe E-Mail-Anwendungen	22
Cloud-basierte Speicherdienste	22
Apps zur Synchronisierung	22

Thema		Kapitel
	Cloud-basierte Anwendungen	22
	Anwendungen für Smartphones/Tablets	22
	Anwendungen für Laptops/Desktops	22
	Virtueller Desktop	22
	Virtuelle Netzwerkkarte	22
4.2	Einrichtung und Konfiguration clientseitiger Virtualisierung	
	Zweck virtueller Maschinen	22
	Erforderliche Ressourcen	22
	Anforderungen für einen Emulator	22
	Sicherheitsanforderungen	22
	Anforderungen an das Netzwerk	2
	Hypervisor	22
5.0	**Fehlerbehebung bei Hardware- und Netzwerkproblemen**	
5.1	Verfolgen Sie die Best-Practice-Methoden, um Probleme zu beheben.	
	Beachten Sie stets die Unternehmensrichtlinien, Verfahrensweisen und Auswirkungen, bevor Sie Änderungen umsetzen.	1
	1. Identifizieren Sie das Problem.	1
	Befragen Sie den Benutzer und stellen Sie fest, ob er Veränderungen am Computer vorgenommen hat. Führen Sie eine Datensicherung durch, bevor weitere Veränderungen stattfinden.	1
	Erkundigen Sie sich, ob es Änderungen in der Umgebung oder der Infrastruktur gegeben hat.	1
	Überprüfen Sie System- und Anwendungsprotokolle (Logdateien).	1
	2. Stellen Sie eine Theorie der wahrscheinlichsten Ursache auf (und hinterfragen Sie das Offensichtliche).	1
	Stellen Sie anhand der Symptome externe oder interne Nachforschungen an, falls erforderlich.	1
	3. Prüfen Sie die Theorie, um die Ursache zu bestimmen.	1
	Falls sich die Theorie bestätigt, legen Sie die nächsten Schritte zur Fehlerbehebung fest.	1
	Sollte sich die Theorie nicht bestätigen, stellen Sie eine neue Theorie auf oder eskalieren Sie das Problem.	1
	4. Erstellen Sie einen Plan zur Lösung des Problems und setzen Sie ihn um.	1
	5. Überprüfen Sie, ob das System vollständig funktioniert, und treffen Sie bei Bedarf vorbeugende Maßnahmen.	1
	6. Dokumentieren Sie die Befunde, die getroffenen Maßnahmen und die Ergebnisse.	1
5.2	Beheben Sie Probleme im Zusammenhang mit Mainboard, RAM, CPUs und Stromversorgung durch geeignete Maßnahmen	
	Symptome	
	Unerwartete Neustarts	3
	Systemabstürze	3, 4
	POST-Piepscodes	5

Thema	Kapitel
Leerer Bildschirm beim Start	4, 16
Uhrzeit und BIOS-Einstellungen werden zurückgesetzt	5
Startversuche vom falschen Laufwerk	16
Ständige Neustarts	16
Keine Stromversorgung	6
Überhitzung	3, 7
Laute Geräusche	6
Unregelmäßiger Ausfall von Geräten	6, 7
Statusanzeigen	6
Keine Stromversorgung trotz drehender Lüfter	6
Rauch oder Qualm	7
Brandgeruch	7
Blue Screen	3, 16
Aufgequollene oder geplatzte Kondensatoren	6
Einträge in den Logdateien und Fehlermeldungen	11
5.3 Beheben Sie Probleme im Zusammenhang mit Festplatten und RAID-Verbünden	
Symptome	9
Schreib-/Lesefehler	9
Geringe Geschwindigkeit	9
Laute Klickgeräusche	9
Systemstart schlägt fehl	9
Laufwerk wird nicht erkannt	9
Betriebssystem wird nicht gefunden	9
RAID-Verbund wird nicht gefunden	9
RAID-Verbund funktioniert nicht mehr	9
Blue Screen	9
S.M.A.R.T.-Fehlermeldungen	9
5.4 Beheben Sie gängige Probleme im Zusammenhang mit Grafikkarte, Projektor oder Bildschirm durch geeignete Maßnahmen	
Symptome	
VGA-Modus	17
Keine Bildanzeige	17
Abschaltung durch Überhitzung	17
Defekte Pixel	17
Bildartefakte	17
Fehlerhafte Farbdarstellung	17
Dunkles Bild	17
Flackerndes Bild	17

Thema	Kapitel
Verzerrtes Bild	17
Eingebranntes Bild	17
Übergroße Bilder und Icons	17
Fehlermeldungen in den Logdateien	17
5.5 Finden und reparieren Sie gängige bei mobilen Geräten auftretende Probleme durch geeignete Maßnahmen	
Symptome	23, 25
Keine Anzeige	23
Dunkle Anzeige	23
Flackernde Anzeige	23
Verklemmte Tasten	23
Unzuverlässige WLAN-Verbindung	23
Akku wird nicht geladen	23
Geisterbilder des Mauszeigers	23
Keine Stromversorgung	23
Statusanzeige der Taste `Numlock`	23
Keine WLAN-Verbindung	23
Keine Bluetooth-Verbindung	23
Anzeige auf externem Bildschirm funktioniert nicht	23
Touchscreen reagiert nicht	25
Apps starten nicht	25
Geringe Geschwindigkeit	25
E-Mail-Entschlüsselung funktioniert nicht	25
Extrem kurze Akkulaufzeit	25
Überhitzung	25
System reagiert nicht	25
Keine Tonausgabe	25
GPS funktioniert nicht	25
Aufgequollener Akku	25
Auseinandernehmen und Zusammenbauen des Geräts	23
Notieren aller Positionen von Kabeln und Schrauben	23
Beschriftung der Bauteile	23
Dokumentation des Herstellers	23
Einsatz geeigneter Werkzeuge	23
5.6 Beheben Sie Druckerprobleme	
Symptome	26
Schlieren oder Streifen	26

Thema	Kapitel
Blasse Ausdrucke	26
Geisterbilder	26
Toner wird nicht auf dem Papier fixiert	26
Zerknittertes Papier	26
Papier wird nicht eingezogen	26
Papierstau	26
Keine Verbindung	26
»Hieroglyphen«, unlesbare Zeichen	26
Vertikale Streifen auf den Ausdrucken	26
Stau in der Druckerwarteschlange	26
Fehlermeldung »Speicherüberlauf«	26
Fehlermeldung »Zugriff verweigert«	26
Drucker druckt nicht	26
Drucker gibt Farben fehlerhaft aus	26
Drucker lässt sich nicht installieren	26
Fehlercodes	26
Ausgabe leerer Seiten	26
Display am Drucker zeigt nichts an	26
5.7 Beheben Sie gängige Probleme in drahtlosen und kabelgebundenen Netzwerken	
Symptome	19–21
Verbindung funktioniert nur sporadisch	21
Nicht verfügbare Ressourcen	21
Internet	21
Lokale Ressourcen	19
Keine Verbindung	19
Freigaben	19
Drucker	19
E-Mail	19
Keine Verbindung	19, 21
APIPA oder link-lokale Adresse	19, 21
Unregelmäßig funktionierende Verbindung	19
IP-Adresskonflikt	19
Geringe Datenübertragungsrate	21
Schwaches Funksignal	20
SSID wird nicht gefunden	20

A.2 Zielzuordnung für CompTIA A+ 220-1002

Thema	Kapitel
1.0 Betriebssysteme	
1.1 Vergleich und Gegenüberstellung der Funktionen und Systemanforderungen verschiedener Betriebssysteme und deren Zweck	
32-Bit und 64-Bit	2, 3
Obergrenzen für das verwendbare RAM	3, 4
Software-Kompatibilität	3, 14
Betriebssysteme für Arbeitsplatzrechner	2
Microsoft Windows	2
Apple Macintosh OS	2
Linux	2
Betriebssysteme für Smartphones/Tablets	2
Microsoft Windows	24
iOS	24
Chrome OS	23
Herstellerspezifische Einschränkungen	
End-of-Life	11
Einschränkungen bei Updates	11
Kompatibilität von Betriebssystemen	11
1.2 Vergleich und Gegenüberstellung der Merkmale verschiedener Windows-Versionen	
Windows 7	2
Windows 8	2
Windows 8.1	2
Windows 10	2
Anforderungen von Unternehmen und Privatpersonen	
Domänenzugriff	11
BitLocker	1
BranchCache	11
EFS	11
Desktop-Einstellungen/Bedienoberfläche	11
1.3 Installation und Aktualisierung des Betriebssystems	
Boot-Verfahren	11
USB	11
CD-ROM	11
DVD	11
PXE	11

Thema	Kapitel
SSD/Flash-Speicherlaufwerke	11
Netboot	11
Externe/Hot-swappable-Laufwerke	11
Interne Laufwerke (Partition)	11
Installationstypen	11
Unbeaufsichtigte Installation	11
Upgrade	11
Neuinstallation	11
Reparaturinstallation	16
Multiboot	11
Installation über das Netzwerk	11
Systemabbild verwenden	11
Wiederherstellungspartition	11
Auffrischen/Wiederherstellen	11, 14
Partitionierung	9
Dynamische Datenträger	9
Basisfestplatte	9
Primäre Partition	9
Erweiterte Partition	9
Logische Laufwerke	9
GPT	9
Dateisystemtypen/Formatierung	
ExFAT	9
FAT32	9
NTFS	9
CDFS	10
NFS	21
ext3, ext4	9
HFS	9
Swap-Partition	9
Schnellformatierung und vollständige Formatierung	9
Bei Bedarf alternative Treiber von Drittanbietern laden	11
Arbeitsgruppe vs. Domäne	11
Einstellung von Datum, Uhrzeit, Region und Sprache	11
Treiberinstallation, Software- und Windows-Updates	11, 14
Wiederherstellungspartition	9
Korrekt formatiertes/partitioniertes Startlaufwerk	11

Thema	Kapitel
Systemanforderungen/Hardware-Kompatibilität	11
Kompatibilität von Anwendungen	11
Betriebssystemkompatibilität/Aktualisierung	11
1.4 Verwendung von Kommandozeilenbefehlen (Miscrosoft)	
Navigation	15
dir	15
cd	15
..	15
ipconfig	19
ping	19
tracert	19
netstat	21
nslookup	19
shutdown	15
dism	11
sfc	15
chkdsk	15
diskpart	16
taskkill	16
gpupdate	15
gpresult	15
format	16
copy	15
xcopy	15
robocopy	15
net use	19
net user	16
[Befehlsname] /?	15
Befehle als Administrator/Hauptbenutzer ausführen	15
1.5 Verwendung von Funktionen und Dienstprogrammen des Betriebssystems (Microsoft)	
Administration	
Verwaltung	13
Geräte-Manager	2, 6, 10, 14, 16, 20
Lokale Benutzer und Gruppen	13
Lokale Sicherheitsrichtlinie	27
Leistungsüberwachung	12

Thema	Kapitel
Dienste	12
Systemkonfiguration	14, 16
Aufgabenplanung	14
Komponentendienste	12
ODBC-Datenquellen	12
Druckerverwaltung	26
Windows Speicherdiagnose	4, 16
Windows Firewall	27
Windows Firewall mit erweiterter Sicherheit	27
Ereignisanzeige	16, 27
Verwaltung von Benutzerkonten	13
MSConfig	14, 16
Allgemein	14
Boot	14, 16
Dienste	14
Systemstart	14
Tools	14
Task-Manager	12, 14, 16
Anwendungen	12
Prozesse	12, 16
Leistung	12
Netzwerk	12
Benutzer	12
Datenträgerverwaltung	8, 9
Laufwerksstatus	9
Bereitstellungspunkte	9
Initialisierung	9
Partitionen erweitern	9
Partitionen aufteilen	9
Partitionen verkleinern	9
Zuweisung und Ändern von Laufwerksbuchstaben	9
Laufwerke hinzufügen	9
RAID-Verbunde hinzufügen	9
Speicherplätze	9
Systemwerkzeuge	
Regedit	12
Eingabeaufforderung	15

Thema	Kapitel
Services.msc	12
MMC	14
MSTSC	21
Notepad	15
Explorer	2, 13, 15, 19
Msinfo32	14
DxDiag	17
Defragmentierung	9, 14
Systemwiederherstellung	14, 16
Windows Update	14
1.6 Verwendung der Systemsteuerung (Microsoft)	
Internetoptionen	21
Verbindungen	21
Sicherheit	21
Allgemein	21
Datenschutz	21
Programme	21
Erweitert	21
Anzeige/Anzeigeeinstellungen	17, 23
Auflösung	17
Farbtiefe	17
Bildwiederholrate	17
Benutzerkonten	13
Ordneroptionen	2
Versteckte Dateien anzeigen	2
Erweiterungen ausblenden	2
Allgemeine Optionen	2
Ansicht	2
System	
Leistung (virtueller Arbeitsspeicher)	14
Remoteeinstellungen	21
Computerschutz	27
Windows Firewall	27
Energieoptionen	23
Energiesparmodus	23
Energiesparpläne	23

Thema	Kapitel
Ruhezustand/Aufwecken	23
Standby	23
Anmeldeinformationsverwaltung	21
Programme und Features	14, 17, 22
Heimnetzgruppe	19
Geräte und Drucker	14, 26
Sound	10
Problembehandlung	16
Netzwerk- und Freigabecenter	19, 21
Geräte-Manager	2, 6, 10, 14, 16, 20
BitLocker	13
Synchronisierungscenter	23
1.7 Installation und Konfiguration von Programmen	
Systemanforderungen	14
Festplattengröße	14
RAM	14
Anforderungen des Betriebssystems	14
Kompatibilität	14
Installationsmethoden und deren Umsetzung	14
Lokal (CD/USB)	14
Netzwerk-basiert	14
Lokale Berechtigungen von Benutzern	14
Ordner- und Dateizugriff für die Installation	14
Überlegungen zur Sicherheit	14
Auswirkungen auf das Gerät	14
Auswirkungen auf das Netzwerk	14
1.8 Einrichtung und Konfiguration des Netzwerks unter Windows	
Heimnetzgruppe und Arbeitsgruppe	19
Einrichtung einer Domäne	19
Netzwerkfreigaben/Administrative Freigaben, Laufwerkszuordnung	13, 19
Druckerfreigaben und Netzwerkdrucker	19, 26
Einrichtung von Netzwerkverbindungen	19–21
VPN	21
Einwahlverbindungen	21
Drahtlose Netzwerke	20
Kabelgebundene Netzwerke	19
WWAN (Mobilfunk)	21

Thema	Kapitel
Proxy-Einstellungen	21
Remotedesktopverbindung	21
Remoteunterstützung	21
Heimnetzwerk, Arbeitsplatznetzwerk und öffentliches Netzwerk	27
Firewall-Einstellungen	27
Ausnahmen	27
Konfiguration	27
Aktivieren/Deaktivieren der Firewall	27
Konfiguration einer alternativen IP-Adresse in Windows	19
IP-Adressierung	19
Subnetzmaske	19
DNS	19
Gateway	19
Eigenschaften von Netzwerkkarten	19
Halb- und Vollduplex, Automatik	19
Geschwindigkeit	19, 20
Wake-on-LAN	19
QoS	19
BIOS (Mainboard-NIC)	19
1.9 Gängige Features und Funktionalitäten der Betriebssysteme macOS und Linux	
Bewährte Verfahrensweisen	
Geplante Datensicherungen	14
Geplante Datenträgerprüfung	14
System-Updates und App Store	14
Patch-Verwaltung	14
Treiber- und Firmware-Aktualisierung	14
Aktualisierung von Anti-Malware-Software	27
Tools	
Backup/Time Machine	14
Wiederherstellung/Snapshots	14
Wiederherstellung von Laufwerksabbildern	16
Datenträgerprüfung und Defragmentierung	14
Shell/Terminal	14
Bildschirmfreigabe	21
Programme sofort beenden	16
Features	
Mehrere Schreibtische/Mission Control	2

Thema	Kapitel
Schlüsselbund	24
Spotlight	15
iCloud	24
Gesten	10
Finder	2
Entfernte CD/DVD	10
Dock	2
Boot Camp	11
Grundlegende Linux-Befehle	
ls	15
grep	15
cd	15
shutdown	15
pwd und paswd	15
mv	15
rm	15
chmod	13
chown	13
iwconfig/ifconfig	15
ps	15
su/sudo	15
apt-get	15
vi	15
dd	15
kill	15, 16
2.0 Sicherheit	
2.1 Physische Sicherheitsmaßnahmen	
Personenschleusen	27
Kartenleser	27
Smartcard	27
Sicherheitspersonal	27
Türschlösser	27
Biometrie	27
Sicherheits-Token	27
Sicherungskabel	27
Server-Sicherungen	27
USB-Anschlusssicherungen	27

Thema	Kapitel
Sichtschutz für Bildschirme	27
RFID-Schlüsselanhänger	27
Führen von Besucherlisten	27
2.2 Computersicherheit	
Active Directory	
Anmeldeskript	19
Domäne	19
Gruppenrichtlinien	27
Organisationseinheiten	19, 27
Home-Verzeichnisse	19
Ordnerumleitung	19
Software-Token	27
MDM-Richtlinien	25
Gesperrte Ports	27
MAC-Adressfilter	27
Zertifikate	27
Antivirussoftware, Anti-Malware	27
Firewalls	27
Benutzerauthentifizierung, sichere Kennwörter	13, 25, 27
Mehrfaktor-Authentifizierung	25, 27
Zugriffsrechte auf Verzeichnisse	27
VPN	21, 24, 27
DLP	27
Zugriffssteuerungslisten	9, 27
Smartcards	27
E-Mail-Filter	27
Vertrauenswürdige Quellen für Software	27
Prinzip der minimalen Rechtegewährung	27
2.3 Vergleich und Gegenüberstellung von drahtlosen Netzwerkprotokollen und Authentifizierungsverfahren	
Protokolle und Verschlüsselung	20
WEP	20
WPA	20
WPA2	20
TKIP	20
AES	20

Thema	Kapitel
Authentifizierung	
Ein-Faktor-Authentifizierung	25, 27
Mehrfaktor-Authentifizierung	25, 27
RADIUS	20
TACACS	20
2.4 Erkennung und Entfernen von Malware und Ergreifen vorbeugender Maßnahmen	
Malware	
Ransomware	27
Trojaner	27
Keylogger	27
Rootkits	27
Viren	27
Botnet	27
Würmer	27
Spyware	27
Werkzeuge und Verfahren	27
Antivirussoftware	27
Anti-Malware	27
Wiederherstellungskonsole	27
Sichern/Wiederherstellen	27
Anwenderschulung	27
Software-Firewalls	27
SecureDNS	27
2.5 Vergleich und Gegenüberstellung von Social Engineering Bedrohungen und Schwachstellen	
Social Engineering	
Phishing	27
Spear Phishing	27
Auftreten als jemand anderes	27
Ausspähen von Kennwörtern bei der Eingabe	27
Tailgating	27
Dumpster Diving	27
DDoS	27
DoS	27
Zero-Day-Angriffe	27
Man-in-the-middle-Angriffe	27
Brute-Force-Angriffe	27
Wörterbuchangriffe	27

Thema	Kapitel
Rainbow Tables	27
Spoofing	27
Nicht-konforme Systeme	27
Zombie	27
2.6 Grundlegende Sicherheitseinstellungen des Betriebssystems (Windows)	
Benutzer und Gruppen	13
Administrator	13
Hauptbenutzer	13
Gast	13
Standardbenutzer	13
NTFS und Freigabeberechtigungen	13, 19
Zugriff gestatten oder untersagen	13
Verschieben und Kopieren von Dateien und Ordnern	13
Dateiattribute	19
Datei- und Ordnerfreigaben	13
Administrative und lokale Freigaben	13
Propagieren von Berechtigungen	13
Vererbung	13
Systemdateien und -ordner	14
Benutzerauthentifizierung	19
Single-Sign-On	19
Ausführen als Administrator oder Standardbenutzer	13
BitLocker	13
BitLocker To Go	13
EFS	13
2.7 Umsetzen bewährter Verfahren zum Schutz von Arbeitsplatzrechnern	
Best Practices beim Einrichten von Kennwörtern	
Verwendung sicherer Kennwörter	13
Ablaufende Kennwörter	13
Kennwortgeschützter Bildschirmschoner	27
BIOS/UEFI-Kennwort	5
Notwendigkeit von Kennwörtern	13
Benutzerkontenverwaltung	
Zugriffsrechte beschränken	27
Anmeldung zeitlich beschränken	27
Gastbenutzerkonten deaktivieren	27
Sperre bei zu vielen fehlgeschlagenen Anmeldeversuchen	27

Thema	Kapitel
Automatische Aktivierung des Bildschirmschoners mit Kennwortschutz	27
Standardbenutzernamen und -kennwörter ändern	13
Grundlegende Active-Directory-Funktionen	19
Benutzerkonto erstellen	19
Benutzerkonto löschen	19
Kennwort zurücksetzen/Sperre aufheben	19
Benutzerkonto deaktivieren	19
Autorun deaktivieren	27
Datenverschlüsselung	27
Patchen und Aktualisieren	14, 27
2.8 Methoden zum Schutz von mobilen Geräten	
Gerätesperren	25
Entsperrung durch Fingerabdruckscanner	25
Entsperrungen durch Gesichtserkennung	25
Entsperrung durch Zeichnen eines Musters	25
Entsperrung durch Kennwort/PIN	25
Remote Wipe	25
Apps zum Lokalisieren des Geräts	25
Backup in der Cloud	25
Restriktionen bei mehrfach gescheiterter Anmeldung	25
Antivirussoftware, Anti-Malware	25
Aktualisierung des Betriebssystems	25
Biometrische Authentifizierung	25
Vollständige Verschlüsselung des Geräts	25
Mehrfaktor-Authentifizierung	25
Anwendungen zur Authentifizierung	25
Vertrauenswürdige und nicht vertrauenswürdige Quellen	25
Firewalls	25
Richtlinien und Verfahren	25
BYOD vs. firmeneigene Geräte	25
Bewertung der Sicherheitsanforderungen	25
2.9 Anwendung der angemessenen Methoden zur Datenvernichtung	
Physische Zerstörung	11
Schredder	11
Bohrer/Hammer	11
Entmagnetisierung	11
Verbrennen/Einschmelzen	11

Thema	Kapitel
Zertifikat der Datenvernichtung	11
Sicheres Löschen von Datenträgern	11
Normale und Low-Level-Formatierung	11
Überschreiben	11
Laufwerke löschen	11
2.10 Schutz kabelgebundener und drahtloser Büro- oder Heimnetzwerke	
Drahtlose Netzwerke	20
SSID ändern	20
Verschlüsselung aktivieren	20
SSID-Übertragung deaktivieren	20
Platzierung von Antennen und Zugriffspunkt	20
Sendeleistung	20
WPS	20
Standardbenutzernamen und -kennwörter ändern	20, 21
MAC-Filterung aktivieren	20
Zuweisung statischer IP-Adressen	20, 21
Firewall-Konfiguration	27
Portweiterleitung und -zuweisung	27
Ports sperren	27
Inhalte filtern/Kindersicherung aktivieren	27
Aktualisierung der Firmware	27
Physischer Schutz	27
3.0 Software-Fehlerbehebung	
3.1 Beheben Sie Probleme des Betriebssystems durch geeignete Maßnahmen (Windows)	
Symptome	16
Geringe Geschwindigkeit des Systems	16
Eingeschränkte Netzwerkverbindung	16
Systemstart schlägt fehl	16
Betriebssystem nicht gefunden	16
Programmabstürze	16, 27
Blue Screen	16
Black Screen	16
Probleme beim Drucken	16
Dienste starten nicht	16
Langsamer Systemstart	16
Langsames Laden von Profilen	16

Thema	Kapitel
Lösungen	16
Defragmentierung der Festplatte	16
Neustart	16
Prozesse beenden	16
Dienste neu starten	16
Netzwerkeinstellungen aktualisieren	16
Systemabbild wiederherstellen	16
Zu älteren Gerätetreibern zurückkehren	16
Aktualisierungen einspielen	16
Bootreihenfolge aktualisieren	16
Dienste/Anwendungen deaktivieren	16
Start im abgesicherten Modus	16
Windows-Profile neu erstellen	16
3.2 Beheben Sie Sicherheitsprobleme durch geeignete Maßnahmen und bewährte Verfahrensweisen	
Symptome	27
Pop-ups	27
Browserumleitung	27
Sicherheitswarnmeldungen	27
Geringe Geschwindigkeit	27
Probleme mit der Internetverbindung	27
Rechner friert ein	27
Programmabstürze	27
Windows-Update schlägt fehl	27
Schurken-Anti-Malware	27
Spam	27
Umbenannte Systemdateien	27
Verschwundene Dateien	27
Geänderte Zugriffsrechte	27
Gekaperte E-Mail-Konten	27
Benachrichtigungen wegen merkwürdiger E-Mail	27
Abwesenheitsnotizen von Unbekannten	27
Fehlermeldung »Zugriff verweigert«	27
Ungültige Zertifikate	27
Fehlermeldungen in System und Anwendungsprotokollen	27
3.3 Bewährte Vorgehensweisen beim Entfernen von Malware	
1. Malware-Symptome erkennen	27
2. Infizierte Systeme isolieren	27

Thema	Kapitel
3. Systemwiederherstellung deaktivieren (Windows)	27
4. Infizierte Systeme bereinigen	27
a) Anti-Malware-Software aktualisieren	27
b) Suchen und entfernen (Abgesicherter Modus und Vorinstallationsumgebung)	27
5. Scans planen und Updates einspielen	27
6. Systemwiederherstellung aktivieren (Windows)	27
7. Anwenderschulung	27
3.4 Finden und beheben Sie bei mobilen Geräten auftretende Probleme durch geeignete Maßnahmen	
Symptome	25
Keine Anzeige oder sehr dunkle Anzeige	25
Unzuverlässige WLAN-Verbindung	25
Keine WLAN-Verbindung	25
Keine Bluetooth-Verbindung	25
Anzeige auf externem Bildschirm funktioniert nicht	25
Touchscreen reagiert nicht	25
Apps starten nicht	25
Geringe Geschwindigkeit	25
E-Mail-Entschlüsselung funktioniert nicht	25
Extrem kurze Akkulaufzeit	25
Überhitzung	25
System reagiert nicht	25
Keine Tonausgabe	25
Ungenaue Reaktion des Touchscreens	25
System gesperrt	25
Apps erzeugen Fehlermeldungen in Logdateien	25
3.5 Finden und beheben Sie gängige bei mobilen Geräten auftretende Sicherheitsprobleme durch geeignete Maßnahmen	
Symptome	25
Signalverlust/schwaches Signal	25
Geringe Akkulaufzeit	25
Geringe Datenübertragungsrate	25
Ungewollte WLAN-Verbindung	25
Ungewollte Bluetooth-Kopplung	25
Verlust persönlicher Dateien/Daten	25
Überschreiten des Datenkontingents	25
Unautorisierter Zugriff auf Benutzerkonten	25

Thema	Kapitel
Unautorisierter Root-Zugriff	25
Unautorisierter Zugriff auf Ortungsdienste	25
Unautorisierte Aktivierung von Mikrofon/Kamera	25
Hohe Auslastung des Systems	25
4.0 Betriebsabläufe	
4.1 Vergleich und Gegenüberstellung der Richtlinien für die verschiedenen Formen der Dokumentation	
Netzwerktopologiediagramme	28
Wissensdatenbank/interne Artikel	28
Zwischenfallsberichte	28
Gesetzliche Auflagen und Unternehmensrichtlinien	28
Nutzungsbedingungen	28
Kennwortrichtlinie	28
Bestandsverwaltung	28
RFID-Etiketten	28
Barcodes	28
4.2 Richtlinien für das Änderungsmanagement	
Dokumentierte Geschäftsprozesse	28
Zweck der Änderung	28
Umfang der Änderung	28
Risikoanalyse	28
Für die Änderung planen	28
Benutzerakzeptanz	28
Änderungsausschuss	28
Genehmigung	28
Rückzugsplan	28
Änderungsdokumentation	28
4.3 Katastrophenvorbeugung und Wiederherstellung	
Sicherung und Wiederherstellung	28
Dateiebene	28
Laufwerksabbilder	28
Wichtige Anwendungen	28
Überprüfung des Backups	28
USV	7, 28
Überspannungsschutz	7, 28
Cloud-Speicher und lokaler Speicher	28
Kontowiederherstellung	28

Thema	Kapitel
4.4 Gängige Sicherheitsmaßnahmen anwenden	
Erdung von Geräten	7
Ordnungsgemäße Lagerung und Handhabung von Geräten	1
Antistatikbeutel	1
Antistatikarmband	1
Antistatikmatten	1
Selbsterdung	1
Umgang mit giftigen Substanzen	
Akkus/Batterien	1, 23, 25
Toner	1, 26
Röhrenmonitore	1, 17
Mobiltelefone und Smartphones	25
Tablets	25
Sicherheitsmaßnahmen	1
Trennen des PCs vom Stromnetz vor der Reparatur	1
Ablegen von Schmuck	1
Hebe- und Tragetechniken	1
Gewichtsgrenzen	1
Brandschutz	1
Kabel ordnungsgemäß verlegen	1, 18
Schutzbrillen	1
Atemschutzmasken	1
Konformität mit Sicherheitsvorschriften	1
4.5 Gefährliche Umgebungsbedingungen und Anwendung von Umweltschutzrichtlinien	
Sicherheitsdatenblatt für den Umgang mit und die Entsorgung von giftigen Substanzen (MSDS, Material Safety Data Sheet)	27
Kontrolle von Temperatur, Luftfeuchtigkeit und Belüftung	27
Spannungsschwankungen, Stromausfälle	7
USV	7
Überspannungsschutz	7
Schutz vor Luftverunreinigungen	27
Staubschutzschränke	27
Luftfilter, Atemschutzmaske	27
Staub und Ablagerungen	26, 27
Druckluft	26, 27
Staubsauger	26, 27
Konformität mit Sicherheitsvorschriften	27, 28

Thema	Kapitel
4.6 Die Grundlagen beim Umgang mit verbotenen Handlungen und Inhalten und Verstößen gegen Richtlinien und Lizenzvereinbarungen	
Reaktion auf Zwischenfälle	27
Erste Maßnahmen	27
Verbotene Handlungen und Inhalte erkennen	27
Berichterstattung	27
Beweissicherung	27
Dokumentation/Dokumentationsänderungen	27, 28
Verwahrungskette	27
Beweismittel schützen/Vorgang dokumentieren	27
Lizenzierung/DRM/EULA	27
Open Source vs. kommerzielle Lizenzen	27
Privatlizenzen vs. Unternehmenslizenzen	27
Datenschutz	27
Persönlich zuweisbare Informationen	27
DSGVO	27
Konformität mit Richtlinien und Vorschriften	27
4.7 Beweisen Sie anhand einer konkreten Situation angemessene Kommunikationsfähigkeit und Professionalität	
Verwenden Sie angemessene Sprache.	1
Meiden Sie Fachjargon, Abkürzungen und Umgangssprache.	1
Zeigen Sie stets eine positive Einstellung.	1
Hören Sie Kunden aufmerksam zu, unterbrechen Sie sie nicht.	1
Seien Sie sich kultureller Unterschiede bewusst.	1
Gebrauchen Sie ggf. akademische Titel.	1
Seien Sie pünktlich.	1
Informieren Sie den Kunden, falls Sie sich verspäten.	1
Vermeiden Sie Ablenkungen.	1
Keine privaten Anrufe	1
Keine SMS, keine sozialen Netzwerke	1
Keine Gespräche mit Kollegen in Gegenwart des Kunden	1
Keine Unterbrechungen aus privaten Gründen	1
Umgang mit schwierigen Kunden oder Situationen	1
Vermeiden Sie es, sich mit Kunden zu streiten.	1
Rechtfertigen Sie sich nicht.	1
Spielen Sie die Probleme des Kunden nicht herunter.	1
Seien Sie nicht wertend.	1

Thema	Kapitel
Klären Sie Kundenaussagen eindeutig.	1
Stellen Sie offene Fragen, um das Problem einzugrenzen.	1
Formulieren Sie das Problem neu, um es zu verstehen.	1
Berichten Sie in sozialen Netzwerken nicht von Ihrer Arbeit.	1
Teilen Sie dem Kunden mit, wie lange Ihre Arbeit dauert.	1
Halten Sie sich an Ihre Vorhersage.	1
Informieren Sie den Kunden über Fortschritte.	1
Bieten Sie verschiedene Reparatur- oder Ersatzmöglichkeiten an.	1
Dokumentieren Sie Ihre Tätigkeit sorgfältig.	1
Sorgen Sie durch Nachfassaktionen für zufriedene Kunden.	1
Behandeln Sie vertrauliches Material von Kunden korrekt.	1
4.8 Grundlagen der Skripterstellung	
Verschiedene Skripttypen	15
.bat	15
.ps1	15
.vbs	15
.sh	15
.py	15
.js	15
Umgebungsvariablen	15
Syntax von Kommentaren	15
Grundlegende Strukturen	15
Einfache Schleifen	15
Variablen	15
Grundlegende Datentypen	15
Integers	15
Strings	15
4.9 Technologien für den Fernzugriff (Remote Access)	
RDP	21
Telnet	21
SSH	21
Programme von Drittanbietern	21
Bildschirmfreigabe	21
File Sharing	21
Überlegungen zur Sicherheit der Zugriffsmethoden	21



Glossar

10BaseT Ethernet-LAN, das Twisted-Pair-Verkabelung erfordert und Datenübertragungsraten von 10 Mbps erreicht.

100BaseT Ethernet-LAN, das Twisted-Pair-Verkabelung erfordert und Datenübertragungsraten von 100 Mbps erreicht. Wird auch als Fast-Ethernet bezeichnet.

1000BaseT Ethernet-LAN, das Twisted-Pair-Verkabelung erfordert und Datenübertragungsraten von 1000 Mbps erreicht. Wird auch als Gigabit-Ethernet bezeichnet.

10-Gigabit-Ethernet (10GbE) Ein Ethernet-Standard, der Datenübertragungsraten von bis zu 10 Gbps erlaubt und für Verbindungen zwischen Servern gebräuchlich ist. Dazu wird CAT6-Ethernet-Kabel oder Glasfaserkabel benötigt.

110-Block Eine Form von Klemmleisten, die zum Anschluss der Horizontalverkabelung an ein Patchfeld verwendet wird.

1.5 Gbps Eine Variante von SATA-Laufwerken mit einem maximalen Datendurchsatz von 150 MBps. Siehe *SATA*.

2.1-Soundsystem Ein Lautsprechersystem, das aus zwei Stereolautsprechern und einem Subwoofer besteht.

2-in-1 Mobile Geräte, die als Laptop und als Tablet dienen sollen.

3 Gbps Eine Variante von SATA-Laufwerken mit einem maximalen Datendurchsatz von 300 MBps. Siehe *SATA*.

3-D-Drucker Geräte zum Erstellen (oder »Drucken«) von dreidimensionalen Objekten, die typischerweise aus einem schmelzbaren Material (wie Kunststofffilamenten) schichtweise aufgebaut werden.

3-D-Grafik Eine Videotechnologie, die versucht, Bilder darzustellen, die ebenso räumlich und strukturiert erscheinen wie echte Objekte.

3G Ein Mobilfunkstandard der dritten Generation (wie EV-DO, UTMS, HSPA+ oder HSDPA), der in der Praxis Datenübertragungsraten von weniger als 10 Mbps erreicht.

40-adriges Flachbandkabel Ein PATA-Kabel, mit dem EIDE-Geräte (wie etwa Festplatten) oder ATAPI-Geräte am Mainboard angeschlossen werden. Siehe auch *PATA*.

4G Ein Mobilfunkstandard der vierten Generation, der vornehmlich in Form von LTE (Long Term Evolution) implementiert ist und theoretisch Datenübertragungsraten von 1 Gbps (beim Download) bzw. 100 Mbps (beim Upload) erreicht.

5.1-Soundsystem Ein Lautsprechersystem, das aus vier Satellitenlautsprechern sowie einem Center-Lautsprecher und einem Subwoofer besteht.

5G Ein Mobilfunkstandard der fünften Generation, der derzeit (Mitte 2019) noch in den Kinderschuhen steckt.

6 Gbps Eine Variante von SATA-Laufwerken mit einem maximalen Datendurchsatz von 600 MBps. Siehe *SATA*.

64-Bit-System Ein System, das kompatible Betriebssysteme wie Windows 7, 8, 8.1 oder 10 und 64-Bit-Anwendungen ausführen kann. 64-Bit-PCs besitzen einen 64 Bit breiten Adressbus und können auf mehr als 4 GB RAM zugreifen.

7.1-Soundsystem Ein Lautsprechersystem, das aus sechs Satellitenlautsprechern (zwei vordere, zwei seitliche, zwei hintere) sowie einem Center-Lautsprecher und einem Subwoofer besteht.

802.11a Ein Standard für drahtlose Netzwerke, der das 5-GHz-Band nutzt und eine theoretische Datenübertragungsrate von 54 Mbps erlaubt.

802.11ac Ein Standard für drahtlose Netzwerke, der das 5-GHz-Band nutzt und MIMO (*Multiple In/Multiple Out*) sowie Multiuser-MIMO verwendet. Die theoretische Datenübertragungsrate beträgt 1 Gbps oder mehr.

802.11b Ein Standard für drahtlose Netzwerke, der das 2,4-GHz-Band nutzt und eine theoretische Datenübertragungsrate von 11 Mbps erzielt.

802.11g Ein Standard für drahtlose Netzwerke, der das 2,4-GHz-Band nutzt und eine theoretische Datenübertragungsrate von 54 Mbps erzielt. Er ist abwärtskompatibel mit 802.11b

802.11n Ein Standard für drahtlose Netzwerke, der sowohl das 2,4- als auch das 5-GHz-Band nutzen kann und MIMO (*Multiple In/Multiple Out*) verwendet. Die maximale theoretische Datenübertragungsrate beträgt mehr als 100 Mbps.

Abbildbereitstellung Installation des Betriebssystems anhand eines vollständigen Systemabbilds einer Festplatte. Äußerst nützlich, wenn das Betriebssystem auf vielen identischen PCs installiert werden soll.

Abgesicherter Modus Ein spezieller Windows-Startmodus zur Diagnose, bei dem nur grundlegende Treiber geladen werden und der virtuelle Arbeitsspeicher nicht aktiv ist.

Absturz Tritt auf, wenn ein Computer oder ein Programm nicht mehr auf Tastendrücke oder andere Eingaben reagiert. Man spricht in diesem Fall davon, dass das Programm »hängt« oder »abgestürzt« ist.

Absturzdauer Die Anzahl der Sekunden, in denen sich ein zu häufig abstürzender Computer in der Luft befindet, nachdem Sie ihn im zweiten Stock aus dem Fenster geworfen haben.

AC (Alternating Current) Siehe *Wechselstrom.*

Accelerometer Ein Beschleunigungssensor, der es Smartphones und Tablets ermöglicht, die Bildschirmausrichtung anzupassen, wenn das Gerät gedreht wird.

ACPI (Advanced Configuration and Power Interface) Eine Spezifikation zur Energieverwaltung, die ihren Vorgänger APM bei Weitem übertrifft., denn sie unterstützt das Anschließen und Entfernen von Geräten im laufenden Betrieb und kann die Energiesparmodi besser steuern.

Ad-hoc-Modus Dezentraler Modus für drahtlose Netzwerke, der auch als Peer-to-Peer-Modus bezeichnet wird. Alle Netzknoten stehen mit allen anderen in Verbindung.

Administrative Freigaben Ein Werkzeug, das lokalen Administratoren Zugriff auf Festplatten und den Systemordner gewährt.

Administratorengruppe Eine Liste der Benutzer, die Administratorrechte besitzen.

Administratorkennwort Zugangsdaten für das Administratorkonto.

Administratorkonto Ein Benutzerkonto, das bei der Erstinstallation des Betriebssystems angelegt wird und vollständigen, ungehinderten Zugriff auf das System gewährt.

Adressbus Ein Satz von Leitungen, der CPU und MCC (normalerweise die Northbridge) verbindet, damit die CPU auf den Arbeitsspeicher zugreifen kann. Der Adressbus wird von der CPU auch zur Ein/Ausgabe genutzt. Bei aktuellen CPUs mit eingebautem MCC bezeichnet der Adressbus die internen elektronischen Verbindungen zwischen CPU und RAM, über den die Adressen der angesprochenen Speicherbereiche übertragen werden. Jeder Speicherplatz besitzt, ähnlich den Postfächern in einem Postamt, eine bestimmte Kennzeichnung, die Speicheradresse. Der Adressbus ermöglicht es dem Mikroprozessor, auf die angegebenen Speicherbereiche zuzugreifen.

Adressraum Die Gesamtheit aller Speicheradressen, die der Adressbus ansprechen kann.

ADSL (Asymmetric Digital Subscriber Line) Ein digitaler Teilnehmeranschluss an das Telefonsystem, der Übertragungsraten von 3 bis mehr als 100 Mbps beim Empfangen und 384 Kbps bis 100 Mbps beim Senden bereitstellt. »Asymmetrisch« weist darauf hin, dass der Empfang von Daten erheblich schneller ist als das Senden.

Adware Bösartige Software, die Reklame herunterlädt und so unerwünschten Datenverkehr erzeugt.

Aero Die Desktop-Umgebung von Windows Vista/7, die einige interessante grafische Effekte mitbringt, etwa Transparenz oder Flip-3D.

AES (Advanced Encryption Standard) Eine Ende der 1990er-Jahre entwickelte Blockchiffre, die eine Blockgröße von 128 Bit und Schlüssel mit einer Länge von 128, 192 oder 256 Bit verwendet, die praktisch nicht zu knacken ist.

AGP (Accelerated Graphics Port) Ein älterer 32/64-Bit-Erweiterungssteckplatz von Intel, der speziell für 66-MHz-Grafik ausgelegt war und einen Datendurchsatz von mindestens 254 Mbps erzielte. Spätere Versionen (2x, 4x, 8x) erreichten einen wesentlich höheren Datendurchsatz.

AHCI (Advanced Host Controller Interface) Eine effiziente Methode, SATA-Host-Bus-Adapter zu verwenden. AHCI ermöglicht einige der fortschrittlichen SATA-Features, wie das Entfernen bzw. Anschließen von Geräten im laufenden Betrieb und NCQ (*Native Command Queuing*, integrierte Befehlsaufreihung).

Aktive Partition Die primäre Partition einer Festplatte, die ein Betriebssystem enthält.

Aktive Leistungsfaktorkorrektur (Active PFC) Ein Schaltkreis in PC-Netzteilen, der Oberschwingungen reduziert.

Aktivierung Der Vorgang, bei dem bestätigt wird, dass die installierte Kopie eines Microsoft-Produkts (zumeist Windows oder eine Anwendung des Office-Pakets) rechtmäßig ist.

Aktivitätsanzeige Eine LED, die durch schnelles Blinken anzeigt, dass eine Netzwerkkarte, ein Hub oder ein Switch Daten über das Netzwerk überträgt.

Aktiv-Matrix Eine Flüssigkristallanzeige, die Passiv-Matrix-Displays weitgehend ersetzt hat und in den meisten Bildschirmen tragbarer Geräte zum Einsatz kommt.

Algorithmus Ein Satz von Regeln zum Lösen einer Aufgabe in einer bestimmten Anzahl von Schritten.

Allgemeine Schutzverletzung Eine Fehlermeldung, die angezeigt wird, wenn mehrere aktive Programme gleichzeitig auf Daten oder Ressourcen zugreifen möchten und es dabei zu einem Konflikt kommt.

ALU (Arithmetic Logic Unit) CPU-Schaltkreise, die grundlegende Rechenoperationen ausführen (Addition, Subtraktion, Multiplikation, Division).

AMD (Advanced Micro Devices) Ein CPU- und Chipsatz-Hersteller, der mit Intel konkurriert. Das Unternehmen produziert CPUs und APUs (*Accelerated Processing Units*) wie FX, die A-Serie, Phenom II, Athlon, Sempron oder Opteron. Unter der Marke ATI stellt das Unternehmen auch Prozessoren für Grafikkarten her.

Ampere (A) Die Maßeinheit des elektrischen Stroms.

Analog Geräte, die den Wert einer Zahl als physikalische Quantität repräsentieren, etwa als Länge oder als elektrische Spannung. Digitale Geräte hingegen verwenden zur Codierung ein System numerischer Einheiten.

AnandTech (`anandtech.com`) Website mit Informationen und Nachrichten zu den Themen Computer, Technologie und Internet.

Android Das Smartphone- und Tablet-Betriebssystem von Google.

Angeheftete Programme In der Task-Leiste abgelegte Programme. Das Symbol eines angehefteten Programms ist ständig in der Task-Leiste sichtbar.

Anmeldebildschirm Der zuerst angezeigte Bildschirm, der zur Anmeldung am System dient.

Anschlagdrucker Siehe *Punktmatrixdrucker*.

Anti-Aliasing Ein Verfahren der Bildbearbeitung, das den starken Kontrast zwischen benachbarten Regionen mildert, z.B. treppenförmige Kanten oder unterschiedliche Farben. Texte und Objekte erscheinen so weniger gezackt. Bei der Verarbeitung von Tonsignalen beschreibt der Begriff das Herausfiltern von Frequenzen oder das Glätten von Wellenformen, etwa wenn digitale Signale wieder in analoge zurückkonvertiert werden.

Antippen Eine Geste, bei der Sie eine Stelle auf dem Touchscreen mit dem Finger berühren, um eine App zu starten oder mit einer laufenden App zu interagieren.

Antistatikarmband Ein spezieller Apparat, der am Handgelenk getragen wird und Potenzialdifferenzen zwischen dem Träger und einem elektronischen Gerät ausgleicht, das auf diese Weise vor elektrostatischen Entladungen geschützt ist.

Antistatikbeutel Ein Beutel aus antistatischem Kunststoff zur Aufbewahrung von elektronischen Komponenten, der das Bauteil vor elektrostatischen Entladungen schützt.

Antistatikmatte Eine spezielle Matte zur Ablage von elektronischen Bauteilen. Sie ist mit einem Erdungskabel verbunden, das dafür sorgt, dass Arbeitsplatz und elektronische Komponenten dasselbe elektrische Potenzial besitzen.

Antiviren-Software Software zur Bekämpfung von Viren, die aktiv nach ihnen sucht und sie entfernt, oder ein System passiv vor Viren schützt.

Antworten entlocken Eine Kommunikationsstrategie, die Technikern dabei hilft, die Probleme eines Benutzers besser zu verstehen. Hören Sie dem Benutzer bei der Beschreibung seines Problems aufmerksam zu und stellen Sie anschließend sinnvolle Fragen.

Anzeige Ein Applet in Windows, um Einstellungen der Anzeige (Auflösung, Bildwiederholrate, Treiberinformationen, Farbtiefe) zu konfigurieren.

API (Application Programming Interface) Eine Schnittstelle zur Beschreibung der von Programmen verwendeten Betriebssystemaufrufe, die durch Konventionen festlegt, wie Dienste genutzt werden.

APIPA (Automatic Private IP Adressing) Ein Windows-Feature, das einem System automatisch eine IP-Adresse zuweist, wenn es keine statische oder per DHCP zugewiesene IP-Adresse besitzt.

APK (Android Application Package) Installationssoftware für Android-Apps.

APM (Advanced Power Management) BIOS-Routinen, die es der CPU ermöglichen, bestimmte Peripheriegeräte ein- oder auszuschalten. Sie wurden 1992 von Intel eingeführt und im Laufe der Zeit fortentwickelt. 1996 wurde APM durch ACPI abgelöst.

App Ein Programm für ein Smartphone oder ein Tablet. Für die Metro-Benutzeroberfläche von Windows 8 ausgelegte Programme werden ebenfalls als App bezeichnet.

App-Scanner Ein Programm, das auf einem Gerät installierte Apps untersucht und auf Risiken hinweist, die mit den Berechtigungen der Apps verbunden sind.

Apple Filing Protocol (AFP) Ermöglicht Macs die gemeinsame Nutzung von Dateien und dient auch zum Erstellen von Backups mit Time Machine über das Netzwerk. Verwendet den TCP-Port 548.

App Store Apples Software-Laden für mobile Geräte. Hier können Sie Apps für Ihr Smartphone, Tablet oder andere Apple-Geräte kaufen.

apt-get Linux-Befehl zum Installieren oder Aktualisieren von Programmen, der auf APT (*Advanced Packaging Tool*) beruht.

Arbeitsbereich Derjenige Bereich, in dem sich bei einer strukturierten Verkabelung die mit dem Netzwerk verbundenen PCs befinden. Dabei handelt es sich oft um einfache Büros oder Arbeitsnischen.

Arbeitsgruppe Siehe *Workgroup*.

Arbeitsplatz Ein Applet, über das der Benutzer auf alle eingebauten oder zusätzlich am System angeschlossenen Laufwerke zugreifen kann und das Teil des Explorers ist.

Archivieren Programme und Daten auf preiswerte Speichermedien (Festplatten, Magnetbänder usw.) kopieren, um sie für einen längeren Zeitraum aufzubewahren.

Archiv-Attribut Das Attribut einer Datei, das anzeigt, ob sie seit der letzten Änderung archiviert wurde. Bei jedem Öffnen, Ändern oder Speichern der Datei wird ihr Archiv-Attribut gesetzt. Eine Backup-Software kann das Archiv-Attribut wieder abschalten und dadurch anzeigen, dass eine Sicherungskopie auf einem anderen Speichermedium vorhanden ist.

ARM Eine energiesparende Prozessorarchitektur, die vor allem bei mobilen Geräten wie Smartphones und Tablets eingesetzt wird.

ARP (**Address Resolution Protokoll**) Ein Protokoll, das zum TCP/IP-Protokollstack gehört und zusammen mit dem gleichnamigen Kommandozeilenprogramm (`arp`) verwendet werden kann, um die einer bestimmten IP-Adresse zugeordnete MAC-Adresse herauszufinden.

Ars Technica (`arstechnica.com`) Website mit Nachrichten zu den Themen Technologie und Internet.

ASCII (**American Standard Code for Information Interchange**) Ein Industriestandard, der einen 8-Bit-Zeichensatz definiert, der aus 96 Zeichen (Groß- und Kleinbuchstaben, Sonderzeichen) und 32 nicht druckbaren Steuerzeichen besteht, die durchgehend nummeriert sind. Der Zeichensatz ist dafür ausgelegt, verschiedenen Computertypen eine einheitliche Druckerausgabe und den Austausch einfacher Textdokumente zu ermöglichen.

ASR (**Automated System Recovery**) Ein Tool von Windows XP, das ein schwer beschädigtes Windows-System wiederherstellen kann. Es besitzt große Ähnlichkeit zur Notfalldiskette in Windows 2000.

AT (**Advanced Technology**) Die Modellbezeichnung für 80286-basierte IBM-Computer der zweiten Generation. Viele der AT-Aspekte, wie z.B. BIOS, CMOS und Erweiterungsbus, sind zu De-facto-Industriestandards geworden. Der physische Aufbau der Komponenten auf dem Mainboard wird als *AT-Formfaktor* bezeichnet.

ATA (**AT Attachment**) Eine Reihe von Festplattenstandards für ältere parallele (PATA) und moderne serielle (SATA) Laufwerke. Siehe auch *PATA* und *SATA*.

ATAPI (**ATA Packet Interface**) Eine Reihe von Standards, die es anderen Speichergeräten als Festplatten ermöglicht, den IDE/ATA-Controller zu verwenden. Verbreitet bei optischen Laufwerken zu finden. Siehe *IDE*.

ATAPI-kompatibel Geräte, die den ATAPI-Standard verwenden. Siehe *ATAPI*.

Atemschutzmaske Eine Maske, die davor schützt, Schmutzpartikel einzuatmen, z.B. beim Zersägen von Trockenbauplatten.

Athlon Bezeichnung einer CPU-Modellreihe des Herstellers AMD.

ATM (**Asynchronous Transfer Mode**) Eine Netzwerktechnologie, die Übertragungsraten zwischen 25 und 622 Mbps ermöglicht und Glasfaserkabel oder UTP-Ethernet-Kabel (CAT5 oder besser) benötigt.

Attribute Eigenschaften einer Datei, die den Status der Merkmale Versteckt, Schreibgeschützt, System oder Archiv festlegen.

ATX (**Advanced Technology Extended**) Ein verbreiteter Mainboard-Formfaktor, der den AT-Formfaktor weitgehend ersetzt hat.

Audio-Interface Eine Soundkarte der Spitzenklasse in einem externen Gehäuse, wie sie Tontechniker und Musiker gern verwenden.

Aufgabenplanung Ein Windows-Werkzeug, das es dem Benutzer ermöglicht, Aufgaben zu bestimmten Zeitpunkten automatisch ausführen zu lassen.

Aufgeplatzte Kondensatoren Defekte Kondensatoren auf dem Mainboard, die oft aufplatzen oder an der Oberseite ausgebeult sind. Dieses Problem trat vor allem Mitte des ersten Jahrzehnts dieses Jahrhunderts auf, als die Hersteller große Mengen defekter Kondensatoren auf den Markt brachten.

Auflösung Ein Merkmal zur Beschreibung von Monitoren und Druckern, das angibt, wie viele Pixel oder Punkte in horizontaler und vertikaler Richtung darstellbar bzw. druckbar sind. Eine höhere Auflösung bedeutet schärfere Bilder oder Ausdrucke von besserer Qualität.

Aufmerksames Zuhören Zu einer respektvollen Kommunikation gehört aufmerksames Zuhören, gegebenenfalls das Anfertigen von Notizen und sein Gegenüber nicht zu unterbrechen.

Aufrichtigkeit Die Wahrheit sagen – für einen Techniker von großer Bedeutung.

Ausführen-Dialogfeld Ein über das Startmenü zugängliches Dialogfeld, in dem man den Namen eines Programms, eines Ordners, eines Dokuments oder einer Internetressource eingibt, die dann geöffnet wird.

Auslagerungsdatei Ein Speicherbereich auf der Festplatte, in den Windows RAM-Inhalte schreibt, wenn der Arbeitsspeicher knapp wird. Wird auch als *Swap-Datei* oder *virtueller Arbeitsspeicher* bezeichnet.

Authentifizierung Eine Methode, die ein Computer nutzt, um zu ermitteln, wer auf ihn zugreifen darf.

Authentifizierungsfaktor Etwas, das zur Authentifizierung einer Person genutzt werden kann, beispielsweise Wissen (Kennwort), Besitz (Smartcard) oder ein biometrisches Merkmal (Fingerabdruck).

Automatische Erkennung (Autodetection) Die automatische Erkennung von Laufwerken durch das BIOS.

Automatische Updates Ein Feature, das es Windows erlaubt, Updates automatisch aus dem Internet herunterzuladen.

Automatische Wiedergabe (AutoPlay) Eine Windows-Einstellung, die es Windows zusammen mit der Datei `autorun.inf` ermöglicht, Medien automatisch zu erkennen und sie zu verwenden. Siehe *`autorun.inf`*.

Autorisierung Eine Methode, die ein Computer nutzt, um zu ermitteln, welche Aufgaben ein authentifizierter Benutzer erledigen darf.

`autorun.inf` Eine auf manchen Medien gespeicherte Datei, die dafür sorgt, dass ein Programm oder eine Installationsroutine automatisch gestartet wird.

Backside-Bus Ein Satz von Leitungen, der die CPU mit dem Level-2-Cache verbindet. Er wurde erstmals im Pentium Pro eingesetzt. Siehe *Frontside-Bus* und *Externer Datenbus*.

Bandbreite Ein Maß für die Datenmenge, die ein Netzwerk pro Zeiteinheit übertragen kann.

Barcode-Scanner Ein Gerät zum Einlesen von UPC-Barcodes (*Universal Product Code*).

Bash Die Standard-Shell der Kommandozeile von macOS und den meisten Linux-Distributionen.

Basisfestplatte Eine auf »klassische« Weise partitionierte Festplatte mit MBR (*Master Boot Record*) und Partitionstabelle. Siehe auch *Dynamische Datenträger*.

Baud Die Geschwindigkeit von Telefonleitungen in Zyklen pro Sekunde. In den Anfangstagen der telefonischen Datenübertragung entsprach die Baud-Rate oft der Anzahl der pro Sekunde übertragenen Bits. Dank Komprimierung und verbesserten Modulationsverfahren gibt es diese Übereinstimmung jedoch schon lange nicht mehr.

`bcdedit` Ein Kommandozeilenprogramm zur Anzeige des BCD-Stores, der die Startoptionen von Windows enthält.

BD-R (Blu-ray Disc Recordable) Ein Blu-ray-Disc-Format, das es ermöglicht, Daten auf eine leere Disc zu schreiben.

BD-RE (Blu-ray Disc REwritable) Das Blu-ray-Disc-Pendant einer wiederbeschreibbaren DVD, das mehrmaliges Beschreiben derselben Blu-ray-Disc gestattet. Siehe *Blu-ray-Disc*.

BD-ROM (Blu-ray Disc-Read Only Media) Das Blu-ray-Disc-Pendant einer DVD-ROM oder CD-ROM. Siehe *Blu-ray-Disc*.

Befehl Eine Anweisung, die Teil eines Programms ist oder im Terminal eingetippt wird, um eine Operation durchzuführen oder ein Programm zu starten.

Befehlssatz Die Gesamtheit der Maschinensprachebefehle, die ein bestimmter Prozessor versteht.

Begrüßungsbildschirm Siehe *Anmeldebildschirm*.

Beidseitig bestücktes RAM Ein RAM-Modul, das auf beiden Seiten der Platine mit RAM-Bausteinen bestückt ist. Kann nur auf dafür geeigneten Mainboards eingesetzt werden, ist aber sehr verbreitet.

Belichtungstrommel Mit lichtempfindlichen Partikeln beschichteter Aluminiumzylinder, der in Laserdruckern verwendet wird und sich oft im Inneren der Tonerkartusche befindet.

Benutzer (Gruppe) Eine Liste der lokalen Benutzer, denen es unter anderem nicht erlaubt ist, die Registry zu ändern oder auf wichtige Systemdateien zuzugreifen. Einfache Benutzer können zwar Gruppen anlegen, allerdings nur die von ihnen selbst angelegten Gruppen verwalten.

Benutzerdateien Die Standardspeicherorte in Windows für die einem bestimmten Benutzerkonto zugehörigen Inhalte, z.B. Dokumente, Bilder, Musik und Videos.

Benutzerkonto Anhand seines Benutzerkontos identifiziert sich ein Benutzer gegenüber einer Anwendung, einem Betriebssystem oder einem Netzwerk. Es umfasst den vollständigen Namen des Benutzers, das Kennwort, den Benutzernamen, die Gruppenzugehörigkeit und je nach Betriebssystem oder Benutzertyp weitere Angaben. Das Benutzerkonto legt für gewöhnlich außerdem fest, welche Rollen der Benutzer einnehmen kann und welche Berechtigungen er besitzt.

Benutzerkonten (Applet) Ein Applet in der Systemsteuerung, mit dem Sie Änderungen an bestehenden (lokalen oder globalen) Benutzerkonten vornehmen können, das Ihnen außerdem Zugriff auf den Charm (oder in Windows 10 die App) PC-EINSTELLUNGEN gewährt, wenn Sie ein neues Benutzerkonto anlegen möchten.

Benutzerkontensteuerung Ein Windows-Feature, das es einem Standardbenutzerkonto erlaubt, gängige Aufgaben zu erledigen und einen Bestätigungsdialog anzeigt, wenn Standardbenutzer oder Administratoren potenziell schädliche Aktionen ausführen möchten (wie z.B. das Installieren eines Programms).

Benutzeroberfläche Eine visuelle Darstellung des Computers auf dem Bildschirm, die für Benutzer einen Sinn ergibt, und mit der sie den Rechner bedienen. Dabei kann es sich um eine grafische Benutzeroberfläche wie Windows 7 oder um eine Kommandozeile handeln, wie die Windows PowerShell oder die Wiederherstellungskonsole.

Benutzerprofil Einem bestimmten Benutzerkonto zugehörige Einstellungen, die *nicht* davon abhängig sind, an welchem Computer sich der Benutzer anmeldet. Profile ermöglichen es, überall dieselben benutzerdefinierten Umgebungen und Sicherheitseinstellungen zu verwenden.

Benutzerschnittstelle Die Art und Weise, wie eine Software bedient wird.

Bereitstellungspunkt Ein Laufwerk, das für den Benutzer wie ein Ordner auf einem anderen Laufwerk aussieht.

Besitzrechte übernehmen Eine spezielle Berechtigung, um die Kontrolle über eine Datei oder einen Ordner zu übernehmen und gegebenenfalls zu verhindern, dass andere darauf zugreifen können.

Bestandsverwaltung Der Schutz von Geräten und Ausrüstungsgegenständen durch Kennzeichnung mit einem Barcode oder einem RFID-Etikett, um diese im Auge behalten zu können.

Bibliotheken Ein seit Windows 7 verfügbares Feature, das Inhalte von an anderen Speicherorten befindlichen Ordnern an einer leicht zugänglichen Stelle im Explorer bereitstellt. Zu den Standardbibliotheken in Windows gehören Dokumente, Musik, Bilder und Videos.

Bildschirm Siehe *Monitor*.

Bildwiederholfrequenz Gibt an, wie oft pro Sekunde der gesamte Bildschirm neu gezeichnet wird. Die meisten Röhrenmonitore besitzen eine Bildwiederholfrequenz von mindestens 60 Hertz.

Binärzahlen Ein Zahlensystem, das anders als die gewohnten Zahlensysteme mit der Basis 10 (Dezimalzahlen) oder 60 (Uhrzeit) die Basis 2 verwendet. Binärzahlen sind für Computer besonders gut geeignet. Ein elektronischer Schaltkreis, der den Unterschied zwischen zwei Zuständen (Ein/Aus, 1 oder 0) erkennen kann, lässt sich viel einfacher und preiswerter herstellen als einer, der zwischen zehn verschiedenen Zuständen (0 bis 9) unterscheiden müsste.

Biometrische Geräte Geräte, die eine Authentifizierung anhand bestimmter körperlicher Merkmale erlauben (z.B. Netzhaut, Iris, Gesicht oder Fingerabdruck) und dazu irgendeinen Sensor verwenden, etwa einen Fingerabdruckscanner.

BIOS (Basic Input/Output System) Software-Routinen, die klassischerweise auf dem System-ROM eines PCs gespeichert sind und die auch als Firmware betrachtet werden können. Sie handhaben den Systemstart und steuern die Hardware (Festplatten, Tastatur, Monitor usw.).

Bit Eine einzelne Binärzahl. Außerdem alle Werte, die den Zustand »Ein« oder »Aus« annehmen können.

Bit-Tiefe Ein Maß für die Anzahl der Farben oder Töne, die ein Gerät erfassen oder darstellen bzw. wiedergeben kann. Eine größere Bit-Tiefe bedeutet, dass mehr Details erfasst, gespeichert und wiedergegeben werden können.

BitLocker-Festplattenverschlüsselung Eine Software zur Verschlüsselung von Festplatten, die Bestandteil der professionellen Windows-Versionen ist. BitLocker erfordert einen speziellen Chip zum Überprüfen der Hardware, der garantieren soll, dass der Computer nicht manipuliert wurde.

BitTorrent Ein Peer-to-Peer File-Sharing-Programm.

Bluetooth Eine Funktechnologie, die für kleine drahtlose Netzwerke mit bestimmten Aufgaben ausgelegt ist. Sie ist kein Ersatz für ein Ethernet-Netzwerk oder ein WLAN.

Blue-ray-Disc (BD) Ein optisches Medium, das 25 oder 50 GB Daten speichern kann und die DVD ersetzen soll. Stand im Wettbewerb zur HD-DVD.

BNC Ein selten gewordener Koaxial-Stecker, der durch eine Vierteldrehung gesichert wird.

Boot Camp Apples Werkzeug zum Installieren von Windows auf einem Computer mit macOS.

Boot Configuration Data (BCD-Datei) Eine Datei, die Informationen über die verschiedenen auf einem System gespeicherten Betriebssystemversionen und Anweisungen zu deren Start enthält.

Booten Ein Vorgang, der eine automatisierte Routine ausführt, die den Arbeitsspeicher leert, das Betriebssystem lädt und den Computer für die Verwendung vorbereitet. Der Begriff entstammt der bildlichen Vorstellung, sich selbst an der eigenen Stiefelschlaufe (engl. *bootstrap*) aus dem Sumpf zu ziehen. Das Booten ist erforderlich, weil der Arbeitsspeicher seinen Inhalt verliert, sobald der Computer ausgeschaltet wird.

Bootfähiges Laufwerk Ein Laufwerk, das ein funktionierendes Betriebssystem enthält. Dabei kann es sich auch um eine Diskette, einen USB-Speicherstick oder um ein optisches Laufwerk handeln.

`bootmgr` Der Windows-Boot-Manager, der anhand der Informationen in der BCD-Datei (Boot Configuration Data) den Startvorgang steuert.

Bootpartitionstabelle Ein Sektor, der wichtige Informationen über seine Partition enthält, etwa den Speicherort der Bootdateien des Betriebssystems. Er ist für das Laden des Betriebssystems auf einer Partition verantwortlich.

`bootrec` Ein Werkzeug der Windows-Wiederherstellungsumgebung, das den MBR, den Bootsektor oder den BCD-Store reparieren kann. Es ersetzt die Befehle `fixboot` und `fixmbr` aus der Wiederherstellungskonsole von Windows XP und noch älteren Windows-Versionen.

Bootreihenfolge Eine Liste, die festlegt, in welcher Reihenfolge die verfügbaren Speichergeräte nach einem Betriebssystem durchsucht werden. Sie kann im CMOS konfiguriert werden.

Bootsektor Der erste Sektor auf einer Festplatte oder einer Diskette, Spur 0. Die Software im ROM weist den Computer an, das hier befindliche Programm zu laden. Wenn es sich um ein startfähiges Laufwerk handelt, weist das Programm im Bootsektor den Rechner an, das Betriebssystem im Stammverzeichnis des Laufwerks zu laden.

Bootstrap-Loader Ein Codeabschnitt im System-BIOS, der nach einem Betriebssystem und einem gültigen Bootsektor sucht. Sobald er fündig wird, übergibt er die Kontrolle dem Bootsektor und entfernt sich selbst aus dem Arbeitsspeicher.

Botnet Ein Netzwerk von mit Schadsoftware infizierten Computern, das den Befehlen der Entwickler der Schadsoftware gehorcht.

bps (bits per second) Ein Maß für die Datenübertragungsgeschwindigkeit. Ein 56K-Modem kann rund 56.000 Bit pro Sekunde übertragen.

Breitband Im Allgemeinen versteht man darunter eine schnelle, stets verfügbare Verbindung mit einer Datenübertragungsrate, die diejenige von einfachen Telefonleitungen deutlich übertrifft.

Brennen Das Speichern von Daten auf einem beschreibbaren optischen Speichermedium, z.B. einer DVD-R.

Bridge Ein Gerät, das zwei Netzwerke miteinander verbindet und den Datenverkehr nur anhand der Netzknotenadressen weiterleitet, sodass der Datenverkehr zwischen den Netzknoten des einen Netzwerks im anderen Netzwerk nicht sichtbar ist. Eine Ethernet-Bridge beispielsweise verwendet nur die MAC-Adressen. Bridges arbeiten auf der zweiten Ebene des siebenschichtigen OSI-Modells. Die Filterung und Weiterleitung von Paketen beruht auf den MAC-Adressen.

Brillen Spezielle Brillen, die es dem Benutzer ermöglichen, bestimmte Computerfunktionen zu nutzen.

Broadcast Eine Übertragung über das Netzwerk, die an alle Netzknoten adressiert ist.

Browser Ein Programm zum Empfangen und Darstellen von Webseiten.

BSoD (Blue Screen of Death) Der berüchtigte Bildschirm mit einer Fehlermeldung, der erscheint, wenn Windows auf ein irreparables Problem stößt.

BTX (Balanced Technology Extended) Ein Mainboard-Formfaktor, der eine Verbesserung des ATX-Standards darstellt.

Buchse Teil einer Steckverbindung, die einen Stecker aufnimmt.

Bug Ein Programmierfehler, der dazu führt, dass ein Programm fehlerhaft arbeitet, falsche Resultate liefert oder abstürzt. Der Ausdruck wurde geprägt, als bei einem der ersten ENIAC-Computer in den Schaltkreisen ein echtes Insekt entdeckt wurde, das einen Fehler verursachte.

Burn-in-Fehler Ein kritischer Defekt, der vom Hersteller eines Geräts verursacht wurde.

Bus Leitungen, die zwei oder mehr verschiedene elektronische Geräte verbinden, damit sie miteinander kommunizieren können. Der Begriff beschreibt außerdem eine Netzwerk-Topologie, bei der alle Computer an einem einzigen Hauptkabel angeschlossen werden, dem Bus-Kabel.

BYOD (Bring Your Own Device) Eine Vereinbarung der IT-Abteilungen mancher Unternehmen, die es den Benutzern erlaubt, ihre eigenen Smartphones oder andere mobile Geräte statt der firmeneigenen zu verwenden. Außerdem bezeichnet der Begriff eine Vertragsform, die manche Mobilfunkanbieter im Programm haben. Sie kaufen ein nicht subventioniertes Gerät und erhalten dafür im Gegenzug einen günstigeren Tarif.

Byte Eine Einheit, die 8 Bit umfasst – sie ist die fundamentale Einheit für Speicherkapazitäten im PC-Bereich. Ein Byte speichert das Äquivalent zu einem Zeichen. Das Byte dient auch als Einheit für die Kapazität von Massenspeichergeräten.

Cache (Festplatte) Ein spezieller Speicherbereich im RAM, der diejenigen Daten der Festplatte zwischenspeichert, auf die am häufigsten zugegriffen wird. Durch den Einsatz von Cache-Speicher kann die Auslastung des Systems optimiert werden.

Cache (L1, L2 usw.) Ein spezieller schneller Speicher, der normalerweise in der CPU integriert ist und diejenigen Informationen speichert, auf die der Prozessor am häufigsten zugreift.

CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) Eine Authentifizierungsmethode, bei der Bilder, Videos, Töne und andere Medien vom Benutzer identifiziert werden müssen. Für Computer ist es ungleich schwieriger als für Menschen, solche Inhalte zu erkennen, daher sind diese Tests nützlich, um festzustellen, ob ein Mensch oder ein Computer Zugriff erlangen möchte.

CAT5 Ethernet-Kabel der Kategorie 5, einem xxTIA-Standard für UTP-Verkabelung, der Datenübertragungsraten von bis zu 100 Mbps unterstützt.

CAT5e Ethernet-Kabel der Kategorie 5e, einem ANSI/TIA-Standard für UTP-Verkabelung, der Datenübertragungsraten von bis zu 1 Gbps unterstützt.

CAT6 Ethernet-Kabel der Kategorie 6, einem ANSI/TIA-Standard für UTP-Verkabelung, der Datenübertragungsraten von bis zu 10 Gbps unterstützt.

CAT6a Ethernet-Kabel der Kategorie 6a, einer Erweiterung des CAT6-Standards für UTP-Verkabelung, der 10GbE-Netzwerke mit Kabellängen von bis 100 Metern unterstützt.

CAT7 Unterstützt 10-Gbps-Netzwerke (100 Meter lange Segmente); die Abschirmung einzelner Leitungspaare verringert das Übersprechen der Signale und dämpft das Rauschen. CAT7 ist *kein* ANSI/TIA-Standard.

`cd (chdir)` Abkürzung für engl. *change directory*. Sie können mit diesem Befehl das Arbeitsverzeichnis der Eingabeaufforderung ändern.

CD (Compact Disc) Ursprünglich als Nachfolger der Schallplatte aus Vinyl gedacht, wurde sie zusammen mit anderen optischen Datenträgern zur bevorzugten Methode, Musik und Daten dauerhaft zu speichern.

CD-Qualität Audiodaten, die mit einer Abtastrate von 44,1 kHz als 16-Bit-Werte mit zwei Kanälen (Stereo) gespeichert werden.

CDDA (**CD-Digital Audio**) Ein spezielles Format, das die ersten CD-ROMs und alle Audio-CDs verwenden, bei dem die Daten auf Spuren unterschiedlicher Länge verteilt werden. Für Musik ist das Format gut geeignet, für Daten hingegen gar nicht, da keine Fehlerüberprüfung der geschriebenen Daten stattfindet.

CDFS (**Compact Disc File System**) Die Dateistrukturen, Regeln und Konventionen, die beim Speichern von Daten auf einer CD verwendet werden.

CD-R (**CD-Recordable**) Ein beschreibbares CD-Format, das nach dem erstmaligen Beschreiben nicht mehr geändert werden kann.

CD-ROM (**Compact Disc/Read Only Memory**) Ein nur lesbares Format für Audio- und Videodaten. CD-ROMs können von CD-ROM-Laufwerken und abwärtskompatiblen optischen Laufwerken gelesen werden, beispielsweise von DVD- und Blu-ray-Disc-Laufwerken.

CD-RW (**CD-Rewritable**) Ein CD-Format, das wie eine Festplatte mehrfach beschrieben werden kann.

Celeron Eine preiswerte Modellreihe von Intel-CPUs.

CFS (**Central File System**) Eine Methode, alle Speichergeräte innerhalb eines Netzwerks oder eines Unternehmens an zentraler Stelle zusammenzufassen, um den Benutzern einfachen Zugang zu den Daten zu ermöglichen.

CFS (**Command File System, Common File System**) Diese Abkürzung findet sich in der Liste der Akronyme in den Lernzielen der CompTIA A+-Zertifizierungsprüfungen – und sonst nirgends. Auch nach gewissenhafter Suche hat der unerschrockene Autor keinen überzeugenden Hinweis auf die Existenz dieser Technologien gefunden und ist zu der Ansicht gelangt, dass es ausreicht zu wissen, dass CFS für *Command File System* oder *Common File System* stehen kann, um Prüfungsfragen zu diesem Thema zu beantworten.

CCNA (**Certified Cisco Network Associate**) Eine der Zertifizierungen, die Kenntnisse von Cisco-Geräten belegt.

Charms Werkzeuge, die in Windows 8 und 8.1 in der Charm-Leiste verborgen sind, wie z.B. Suche, PC-Einstellungen usw.

Charm-Leiste Hier sind in Windows 8 und 8.1 die Charms zu finden. Bewegen Sie den Mauszeiger in die obere rechte Ecke des Bildschirms, um sie anzuzeigen.

Chipsatz Elektronische Chips, die dafür ausgelegt sind, miteinander zusammenzuarbeiten und alle systemnahen Aufgaben eines PCs erledigen. Der Chipsatz der ersten PCs bestand aus fast 30 verschiedenen Komponenten. In den 1990er- und 2000er-Jahren bestanden Chipsätze aus nur einigen wenigen Chips, die Bestandteil des Mainboards waren. Bei aktuellen CPUs sind die Controller, beispielsweise Speicher- und Grafik-Controller, integriert. Fast alle heutigen »Chipsätze« bestehen aus nur einem Chip.

`chkdsk` (**CheckDisk**) Ein Werkzeug in Windows, das Fehler auf der Festplatte erkennen und in gewissem Maße auch reparieren kann. Ursprünglich handelte es sich um ein DOS-Tool (`chkdsk.exe`), heutzutage trägt aber auch die ausführbare Datei für die grafische Benutzeroberfläche des Werkzeugs zur Fehlerprüfung diesen Namen.

`chmod` Linux-Befehl zum Ändern der Berechtigungen.

`chown` Linux-Befehl zum Ändern des Eigentümers und der Gruppe, zu der eine Datei oder ein Ordner gehört.

Chrome OS Googles Linux-basiertes Betriebssystem, das dafür ausgelegt ist, per Internet auf Google-Dienste wie Gmail, Google Docs und andere zuzugreifen. Chrome OS ist auf zweckbestimmter Hardware (Chromebooks) vorinstalliert.

Chromebook Ein Chromebook ist ein tragbarer Computer, auf dem Googles Linux-basiertes Chrome OS läuft. Chromebooks konzentrieren sich auf Webanwendungen und setzen auf die Nutzung des praktisch unbegrenzten Speicherplatzes in der Cloud und Anwendungen, die als *SaaS* (*Software as a Service*) über das Web bereitgestellt werden. Weil sie den Großteil der Arbeitslast nicht selbst erledigen, haben Chromebooks den Ruf, billig und schlicht zu sein, aber Premium-Chromebooks sind zunehmend gebräuchlich.

CIFS (Common Internet File System) Eine Variante des SMB-Protokolls. Es gilt inzwischen als veraltet, ist aber nach wie vor weit verbreitet.

Client Ein Computerprogramm, das die Dienste eines anderen Computerprogramms nutzt. Der Begriff beschreibt auch Software, die auf von einem Server bereitgestellte Informationen zugreift. Ihr Mobiltelefon ist ein Client, und die Telefongesellschaft ist der dazugehörige Server.

Client/Server Eine Beziehung, in der Client-Software im Namen eines Anwenders die von einem Server bereitgestellten Dienste nutzt.

Client/Server-Netzwerk Ein Netzwerk, in dem fest zugeordnete Server- und Client-Computer vorhanden sind.

Clientseitige Virtualisierung Die Verwendung eines auf einem Client-Rechner installierten Hypervisors zur Ausführung einer virtuellen Maschine. Die VM kann auf dem Client erstellt und gespeichert sein oder sich auf einem Server im Netzwerk befinden.

Closed Source Der Begriff beschreibt Produkte, die vollständig unter der Kontrolle des Entwicklers bzw. Herstellers stehen. Er ist vor allem auf Software anwendbar.

Closed-Source-Software Software, deren Quellcode geheim gehalten wird.

Cloud-Computing Ein Modell, das den Zugriff auf Speicher und andere gemeinsam (oder nicht gemeinsam) genutzte Ressourcen bei Bedarf ermöglicht. Die Cloud beruht auf verschiedenen Diensten wie IaaS, PaaS, SaaS oder einer hybriden Kombination dieser Dienste.

Cluster Windows organisiert Daten in Gruppen (Speichereinheiten), die als Cluster bezeichnet werden, um gewisse Beschränkungen des Dateisystems zu umgehen. Die Clustergröße hängt von der Größe der Datei und der Partition ab.

CMOS (Complementary Metal-Oxide Semiconductor) Das CMOS war ursprünglich ein nichtflüchtiger Speicher, der Informationen über grundlegende Bestandteile des PCs (Festplatte, Diskettenlaufwerke, Menge des Arbeitsspeichers usw.) enthielt. Heutzutage wird zu diesem Zweck nicht-flüchtiger Flash-RAM-Speicher verwendet. Der Inhalt ist der gleiche geblieben und es wird auch noch immer als CMOS bezeichnet, obwohl es sich fast immer eigentlich um Flash-RAM handelt.

CMOS-Batterie Eine Lithium-Ionen-Knopfzelle, die den CMOS-Speicherchip mit Spannung versorgt, wenn der Computer ausgeschaltet ist. Die Batterie ist meistens vom Typ CR2032.

CMOS-Clear Wenn diese Steckbrücke (Jumper) auf dem Mainboard aktiviert ist, wird das CMOS auf Werkseinstellungen zurückgesetzt.

CMOS-Setup-Programm Ein Programm, das es ermöglicht, auf die CMOS-Daten zuzugreifen und sie zu aktualisieren. Für dieses Programm sind auch die Begriffe *System-Setup-Utility* oder *UEFI/BIOS-Setup* geläufig.

CNR (Communications and Networking Riser) Ein proprietärer Steckplatz, der auf manchen Mainboards Modem-, Sound- oder Netzwerkkarten aufnimmt.

Code Ein Satz von Symbolen, die Zeichen repräsentieren (z.B. ASCII-Code) oder die Anweisungen eines Computerprogramms. (Programmierer schreiben Quellcode, der in ein Programm oder in Maschinencode übersetzt werden muss, damit der Computer ihn ausführen kann.)

Codenamen Bezeichnungen, die zur Unterscheidung verschiedener Varianten einer CPU-Modellreihe dienen.

Codec (Compressor/Decompressor) Software, die Streaming-Daten komprimiert oder entkomprimiert.

COM-Ports Anschlüsse zur seriellen Kommunikation. Zur Kennzeichnung werden die Anschlüsse durchnummeriert (COM1, COM2, usw.).

CompactFlash (CF) Ein älteres, aber noch immer verbreitetes Format von Flash-Speicherkarten. Die Schnittstelle ist ein vereinfachter PC-Card-Bus, somit unterstützen CF-Karten auch Ein-/Ausgabegeräte.

CompTIA A+ 220-1001 Die erste Hälfte der CompTIA A+-Zertifizierung für Computertechniker. Die Prüfung 1001 konzentriert sich vornehmlich auf das Verständnis von Terminologie und Technologie sowie darauf, wie grundlegende Arbeiten ausgeführt werden, etwa das Aufrüsten von RAM oder grundlegender Support für Netzwerke und mobile Geräte.

CompTIA A+ 220-1002 Die zweite Hälfte der CompTIA A+-Zertifizierung für Computertechniker. Die Prüfung 1002 konzentriert sich insbesondere auf Software, Sicherheit und Fehlerbehebung.

CompTIA A+-Zertifizierung Eine industrieweite, herstellerunabhängige Zertifizierung, die Computertechnikern ihre Kompetenz bescheinigt.

CompTIA Network+-Zertifizierung Eine industrieweite, herstellerunabhängige Zertifizierung für Netzwerktechniker, die Hardware, Installation und Fehlerbehebung umfasst.

Computer Ein elektronisches Gerät, das Berechnungen durchführen kann.

Computer Standardbenutzerschnittstelle des Explorers; zeigt Festplatten und Laufwerke mit Wechseldatenträgern an.

Computerschutz Ein Windows-Feature, das es gestattet, vorhergehende Versionen von Dateien oder Ordnern wiederherzustellen.

Computerverwaltung Ein Applet in der Windows-Verwaltung, das verschiedene nützliche Snap-Ins enthält, z.B. den Geräte-Manager und die Datenträgerverwaltung.

Computing Technology Industry Association (**CompTIA**) Ein gemeinnütziger Interessenverband, der die Zertifizierungsprüfungen CompTIA A+ und CompTIA Network+ sowie viele weitere herstellerunabhängige IT-Zertifizierungsprüfungen verwaltet.

Containerdatei Eine Datei, die zwei oder mehr separate, komprimierte Spuren enthält, typischerweise eine Audio- und eine Videospur. Für Containerdateien ist auch die Bezeichnung *Wrapper* üblich.

Controller-Karte Eine Adapterkarte, über die Geräte wie Laufwerke an das Mainboard angeschlossen werden.

Convertibles Eine Untermenge von 2-in-1-Geräten, die ein spezielles Scharnier besitzen, sodass sie als Laptop oder als Tablet genutzt werden können.

copy Ein Kommandozeilenbefehl, der eine Kopie einer Datei erstellt und sie an anderer Stelle speichert.

Core Bezeichnung einer Modellreihe von Intel-CPUs, die dem Pentium 4 nachfolgte, z.B. Core i3, Core i5 oder Core i7.

cp Kopierbefehl in Linux.

CPU (**Central Processing Unit**) Das »Gehirn« des Computers. Ein Mikroprozessor, der die Berechnungen des Computers ausführt. CPUs tragen Bezeichnungen wie Core i7 oder Opteron.

CRC (**Cyclic Rednundancy Check**) Eine sehr genaue mathematische Methode, um Fehler bei der Übertragung großer Datenströme zu erkennen. Vor dem Versand errechnet der Absender anhand der Daten eine CRC-Prüfsumme. Der Empfänger berechnet diese Prüfsumme dann ebenfalls. Unterscheiden sich die Werte, sind die Daten während der Übertragung beschädigt worden und werden erneut übermittelt. Ethernet-Pakete setzen den CRC-Algorithmus im FCS-Bereich (*Frame Check Sequence*) des Frames ein.

Crimpzange Ein spezielles Werkzeug, mit dem Twisted-Pair-Kabel an RJ-45-Steckern angeschlossen werden.

cron Ein Werkzeug, das viele Linux-Distributionen verwenden, um geplante Aufgaben auszuführen.

Crossover-Kabel Ein Standard-UTP-Kabel, dessen RJ-45-Stecker an einem Ende nach dem 568A-Standard und am anderen Ende gemäß 568B-Standard belegt sind. Dadurch sind die Leitungen zum Empfangen und Senden an einem Ende vertauscht, und das Kabel simuliert so die Verbindung zu einem Switch.

CRT (**Cathode Ray Tube**) Die Röhre eines Monitors, in der Elektronenstrahlen auf dem phosphoreszierenden Schirm ein Bild erzeugen. Der Begriff wird auch für das Gerät als Ganzes verwendet, wenn es statt eines LCD-Bildschirms eine Röhre verwendet.

CSMA/CA (**Carrier Sense Multiple Access/Collision Avoidance**) Ein Verfahren, das drahtlose Geräte verwenden, um bei der Datenübertragung die bei Funkverbindungen nur schwer erkennbaren Kollisionen von Datenpaketen zu vermeiden.

CSMA/CD (**Carrier Sense Multiple Access/Collision Detection**) Ein Verfahren, das Ethernet-Geräte verwenden, um nach erkannten Kollisionen von Datenpaketen die Daten erneut zu versenden.

D-sub-Anschluss Siehe *DB-Anschluss.*

DAC (Discretionary Access Control) Ein Autorisierungsverfahren, das darauf beruht, dass der Eigentümer einer Ressource nach eigenem Ermessen entscheiden kann, wer darauf zugreifen darf (Zugriffskontrolle nach eigenem Ermessen). Es ist erheblich flexibler als MAC (*Mandatory Access Control*, obligatorische Zugriffskontrolle).

Datei Eine Sammlung von Daten, die nach dem Erledigen einer bestimmten Aufgabe weiterhin gespeichert wird. Eine Datei kann Programmbefehle oder Daten (Zahlen, Text, Grafik) enthalten.

Datei-Explorer Siehe *Explorer.*

Dateiformat Die Art und Weise, in der Informationen in einer Datei gespeichert sind. Die beiden wichtigsten sind Text (ASCII) und das Binärformat (z.B. Bilder), von dem es allerdings oft eine Vielzahl verschiedener Varianten gibt (z.B. BMP, GIF oder JPEG). Typischerweise ist das Dateiformat an der Dateinamenerweiterung erkennbar, beispielsweise `.txt` bei einer Textdatei oder `.exe` bei einem Programm.

Dateiname Der einer Datei beim Anlegen zugewiesene Name. Die Dateien innerhalb eines Ordners müssen eindeutige Namen besitzen. Dateinamen dürfen fast alle Zeichen enthalten, auch Leerzeichen. Nicht erlaubt sind hingegen `\`, `/`, `:`, `*`, `?`, `"`, `<`, `>` und `|`.

Dateinamenerweiterung Zwei, drei, vier, fünf, oder mehr Zeichen, die dem Dateinamen folgen und den Dateityp festlegen. Gängige Dateinamenerweiterungen sind `.zip`, `.exe`, `.doc`, `.java` oder `.xhtml`.

Dateiserver Ein Computer, der Programme, Lernsoftware, Verwaltungswerkzeuge und andere Daten in einem LAN oder WAN bereitstellt. Er »serviert« diese Informationen anderen Computern über das Netzwerk, nachdem sich Benutzer mit ihren Zugangsdaten angemeldet haben.

Dateisystem Ein Schema, das festlegt, wie das Betriebssystem lesend oder schreibend auf die Daten eines Laufwerks zugreifen kann. FAT32 oder NTFS sind Beispiele für Dateisysteme. Siehe *Datenstruktur.*

Dateizuordnung Beschreibt die Zuordnung eines bestimmten Dateityps zu einem Programm, das ihn öffnen kann. Beispielsweise könnte eine `.mp3`-Datei dem Programm Winamp zugeordnet sein.

Datenklassifizierung Ein System, Daten anhand ihrer Bedeutung in verschiedene Kategorien einzuteilen, z.B. als öffentlich, vertraulich oder streng geheim.

Datenroaming Ein Feature des Mobilfunksystems, das einen automatischen Wechsel der Funkzelle und des Mobilfunkanbieters ermöglicht, ohne dass man dies bemerkt.

Datenschutz-Grundverordnung (DSGVO) Eine Verordnung der Europäischen Union, die einen weitreichenden Schutz der persönlichen Daten von EU-Bürgern bietet.

Datenspeicherung Das Erstellen dauerhafter Kopien Ihrer Dokumente, damit Sie später wieder darauf zugreifen können.

Datenstruktur Ein Schema, das festlegt, wie das Betriebssystem lesend oder schreibend auf die Daten eines Laufwerks zugreifen kann. Siehe auch *Dateisystem.*

Datenträger klonen Das Erstellen einer vollständigen Kopie eines Laufwerks, inklusive aller Daten, Software, Konfigurationsdateien, die dann auf einen anderen PC übertragen wird.

Datenträgerbereinigung Zu Windows gehörendes Werkzeug, das dem Benutzer beim Aufräumen auf der Festplatte hilft, indem temporäre Internetdateien, ungenutzte Programme usw. gelöscht werden.

Datenträgerinitialisierung Ein Vorgang, bei dem spezielle Informationen auf die an einem System angeschlossenen Laufwerke geschrieben werden.

Datenträgerkontingente Ein Programm, das es Administratoren ermöglicht, Obergrenzen für den für einzelne Benutzer verfügbaren Speicherplatz auf einem Laufwerk vorzugeben.

Datenträgerverwaltung Ein Applet, zu finden in der Systemsteuerung unter VERWALTUNG|COMPUTERVERWALTUNG, das es Technikern gestattet, die verschiedenen an einem System angeschlossenen Laufwerke zu konfigurieren.

DB-Anschluss D-förmige Anschlüsse, die für eine Vielzahl von Verbindungen eingesetzt werden. Es gibt sowohl männliche (mit Pins, male) als auch weibliche (mit Buchsen, female) DB-Anschlüsse. Sie sind noch recht verbreitet, werden aber nur selten benutzt.

DB-9-Anschluss Ein DB-Anschluss mit zwei Pin-Reihen, der zum Verbinden mit seriellen Geräten verwendet wird (z.B. Modems, Terminalkonsolen oder Switches, die über eine serielle Leitung konfiguriert werden).

DC (Direct Current) Siehe *Gleichstrom.*

dd Linux-Befehl zum Kopieren ganzer blockorientierter Speichergeräte.

DDOS (Distributed Denial of Service) Ein Angriff auf einen Computer oder ein Netzwerk, bei dem viele Computer massenhaft Daten und Anfragen senden und so versuchen, den normalen Betrieb lahmzulegen.

DDR SDRAM (Double Data Rate SDRAM) Ein DRAM-Typ, der bei jedem Taktzyklus zwei Datenbits überträgt. Siehe *DRAM.*

DDR2 SDRAM Ein SDRAM-Typ, der bei jedem Taktzyklus vier Datenbits überträgt. Siehe *DDR SDRAM.*

DDR3 SDRAM Ein SDRAM-Typ, der Daten mit der doppelten Geschwindigkeit von DDR2 SDRAM überträgt.

DDR3L Eine DDR3-Variante, die eine niedrigere Spannung verwendet.

DDR3U Eine DDR3-Variante, die eine noch niedrigere Spannung verwendet.

DDR4 SDRAM Ein SDRAM-Typ, der eine höhere Datendichte und niedrigere Spannungen als DDR3 verwendet und schnellere Datenübertragungsraten beherrscht. Die maximale Speicherkapazität eines DDR4 DIMMs beträgt (theoretisch) 512 GB.

DE (Desktop Environment) Bezeichnung für die zahlreichen Benutzeroberflächen der verschiedenen Linux-Distributionen.

Debuggen Das Aufspüren, Nachverfolgen und Beseitigen von Fehlern in einem Computerprogramm.

Dedizierter Server Ein Computer, der keinerlei Client-Funktionalitäten nutzt, sondern ausschließlich als Server arbeitet.

Definitionsdatei Eine Liste der Signaturen von Viren, die eine Antiviren-Software erkennen kann. Sie sollte häufig aktualisiert werden.

Defragmentierung Ein Vorgang, bei dem die Dateien auf einer Festplatte so umgeordnet werden, dass sich die Bestandteile aller Dateien jeweils in zusammenhängenden Clustern befinden. Dadurch kann schneller auf die Daten zugegriffen werden.

del Kommandozeilenbefehl zum Löschen von Dateien.

Desktop Die meistgenutzte Schnittstelle von Windows-Betriebssystemen.

Desktop-Ersatz Ein tragbarer Computer, der ebenso leistungsfähig wie ein Desktop-Rechner ist. Derartige Systeme sind für gewöhnlich ziemlich schwer und oft deutlich teurer als der Desktop-Rechner, den sie ersetzen sollen.

Dezibel Eine Maßeinheit, die typischerweise zur Beschreibung der Lautstärke verwendet wird. Je größer der Dezibelwert ist, desto lauter ist ein Ton.

DFS (Distributed File System) Eine Umgebung, in der sich die gemeinsam genutzten Daten auf verschiedenen Speichergeräten in mehreren Servern, Clients oder Hosts befinden.

DFÜ (Datenfernübertragung) Die Software, die Windows verwendet, um eine Verbindung zwischen Modem und Internetanbieter herzustellen.

DHCP (Dynamic Host Configuration Protocol)4G Ein Protokoll, über das Clients von einem entsprechend konfigurierten Server automatisch TCP/IP-Einstellungen abfragen können. Verwendet die UDP-Ports 67 und 68.

Dienst Ein im Hintergrund laufendes Programm, das nirgends als Programmsymbol angezeigt wird. Im Task-Manager können Sie sich die laufenden Dienste anzeigen lassen.

Dienste Eine Registerkarte im Task-Manager, auf der die laufenden Dienste des Systems angezeigt werden.

Dienstprogramme Ein Ordner in macOS, der Programme enthält, mit denen Dinge konfiguriert und bewerkstelligt werden können, die mit den normalen Systemeinstellungen nicht machbar sind, z.B. die Aktivitätsanzeige und das Terminal.

Differenzielles Backup Ähnelt einem inkrementellen Backup. Sichert die Dateien, die sich seit dem letzten Backup geändert haben. Das Archiv-Attribut bleibt dabei unangetastet.

Digitalkamera Eine Kamera, die fotografischen Film auf elektronischem Wege simuliert.

Digitales Zertifikat Enthält den öffentlichen Schlüssel, den ein Webserver einem Browser übermittelt, damit er die vom Server bereitgestellten Daten entschlüsseln kann.

Digital signierter Treiber Ein speziell für Windows ausgelegter Treiber, der von Microsoft getestet und zertifiziert wurde. Microsoft bestätigt damit, dass der Treiber stabil funktioniert.

Digitizer (Bildschirm) Die Touchscreen-Technologie, die Berührungen durch Finger oder Eingabestift in Eingaben für das Gerät umwandelt.

Digitizer (Peripheriegerät) Ein Gerät, mit dem man am Computer zeichnen kann. Wird auch als Grafiktablett bezeichnet.

DIMM (Dual Inline Memory Module) 32- oder 64-bittige DRAM-Module, die sich durch die Pinbelegung unterscheiden. DIMMs gibt es in einer Vielzahl verschiedener Größen. Die Varianten mit 184, 240 oder 288 Pins sind bei Desktop-PCs am häufigsten anzutreffen.

DIN (Deutsches Institut für Normung) Ein runder Stecker mit Pins oder Buchsen, der durch das Deutsche Institut für Normung standardisiert wurde. Inzwischen ist dieser Steckertyp weitgehend veraltet, aber DIN- und Mini-DIN-Stecker wurden lange zum Anschließen von Tastaturen, Mäusen, Videosystemen und anderen Peripheriegeräten verwendet.

Dipolantennen Standardantennen (gerade Ausrichtung, wie Teleskopantennen), die für omnidirektionales Empfangen/Senden geeignet sind.

`dir` Kommandozeilenbefehl zur Anzeige des Inhalts des aktuellen Arbeitsverzeichnisses.

DirectX Verschiedene APIs, die es Programmen ermöglichen, multimediale Inhalte zu nutzen (Sound, Video, Grafik). Wird in Windows 7 zur Darstellung des Aero-Desktops verwendet.

Disk-Duplexing Spiegelung einer Festplatte (RAID 1), die jedoch nicht nur zwei Festplatten, sondern auch zwei Controller verwendet; etwas schneller als eine herkömmliche Spiegelung.

Disk-Thrashing Permanenter Festplattenzugriff, weil dem System nicht genügend Arbeitsspeicher zur Verfügung steht. Wenn der Arbeitsspeicher knapp wird, verwendet Windows die Festplatte als virtuellen Arbeitsspeicher und verursacht auf diese Weise die ungewöhnlich hohe Anzahl von Festplattenzugriffen.

Diskette Ein Wechseldatenträger, der zwischen 720 KB und 1,44 MB Daten speichern kann.

Diskettenlaufwerk Ein Gerät, das 3,5-Zoll-Disketten als Wechseldatenträger verwendet.

`diskpart` Ein Kommandozeilenprogramm zur Partitionierung von Festplatten.

DisplayPort Ein digitaler Videoanschluss, den Apples Desktop-Macs und einige PCs, vornehmlich von Dell, verwenden. Er wurde von der VESA entwickelt, um VGA und DVI zu ersetzen.

Distanzbolzen Kleine mechanische Abstandshalter, die am Boden des Computergehäuses festgeschraubt sind. Auf ihnen wird das Mainboard platziert und mit kleinen Schrauben befestigt.

Distribution Eine bestimmte Linux-Variante.

DLP (Data Loss Prevention) Regelsätze, die das versehentliche Bekanntwerden vertraulicher Informationen verhindern sollen, die für gewöhnlich zum Filtern ausgehenden Datenverkehrs eingesetzt werden.

DLP (Digital Light Processing) Eine Anzeigetechnologie, bei der Licht von mikromechanisch gesteuerten Spiegeln auf eine Anzeigeoberfläche geworfen wird.

DMA (Direct Memory Access) Ein Verfahren, mit dem manche PC-Komponenten auf den Arbeitsspeicher zugreifen können, ohne die CPU zu verwenden.

DMA-Controller Befindet sich zwischen dem RAM und der PC-Komponente und verarbeitet DMA-Anfragen.

DMZ (**Demilitarisierte Zone**) Ein kaum oder nicht geschütztes Subnetz, das zwischen der äußeren Firewall und dem hochgradig geschützten internen Netzwerk verortet ist. In einer DMZ werden vornehmlich Server mit öffentlicher IP-Adresse betrieben (wie z.B. Web- oder Mailserver).

DNS (**Domain Name System**) Das TCP/IP-System zur Namensauflösung, das Hostnamen in IP-Adressen übersetzt.

DNS-Domäne Ein bestimmter Zweig des DNS-Namensraums. Zu den Top-Level-Domänen gehören beispielsweise `.com`, `.gov` oder `.edu`.

Dock Eine Leiste am Bildschirmrand des Schreibtischs von macOS, in der man Programmsymbole ablegt, um schnell darauf zugreifen zu können.

Dockingstation Ein Gerät, das einem tragbaren Computer neben weiteren Anschlüssen zusätzliche Features bereitstellt (z.B. ein DVD-Laufwerk oder Kartensteckplätze). Besitzt Ähnlichkeit mit einem Port-Replikator und dient auch als Ladestation für mobile Geräte.

Dokumente Der Windows-Ordner zum Speichern von Dokumenten.

Dokumentieren von Befunden, Maßnahmen und Ergebnissen Aufzeichnen der Problembehebungsfälle: Was war das Problem, wie wurde es behoben und sonstige Informationen. (Schritt 6 der CompTIA-Strategie zur Fehlersuche.)

Dolby Digital Eine Technologie zur Rauschunterdrückung bei digitalen Audioaufnahmen.

Domäne Gruppierungen von Benutzern, Computern oder Netzwerken. In Microsoft-Netzwerken besteht eine Domäne aus Benutzern und Computern, die auf einen gemeinsamen Verzeichnisdienst zugreifen und für die eine einheitliche Sicherheitsrichtlinie gilt. Im Internet beschreibt eine Domäne eine Gruppe von Computern, bei denen ein Teil des hierarchischen Namens übereinstimmt. Es gibt noch weitere Domänentypen, z.B. Broadcast-Domänen.

Domänennetzwerk Ein Netzwerk, das es überflüssig macht, sich an mehreren Servern anmelden zu müssen, indem ein Domänen-Controller die Zugangsdaten aller Systeme verwaltet.

DoS (**Denial od Service**) Ein Angriff auf einen Computer, der den normalen Betrieb lahmlegen soll, normalerweise indem er mit sinnlosen Anfragen überhäuft wird, um ihn dadurch für andere Benutzer unbrauchbar zu machen.

DOS (**Disk Operating System**) Das erste weitverbreitete Betriebssystem für PCs. Dieses textbasierte, nicht-multitaskingfähige Betriebssystem wurde erst mit der Einführung von Windows 95 vollständig ersetzt.

dpi (**dots per inch**) Ein Maß für die Auflösung eines Druckers, das angibt, wie viele Punkte pro Zoll (2,54 cm) in horizontaler Richtung gedruckt werden können.

DRAM (**Dynamisches RAM**) Der in den meisten PCs eingesetzte RAM-Typ. DRAM speichert die Bits in aus Transistoren und Kondensatoren bestehenden Speicherzellen. Da der Kondensator einer DRAM-Speicherzelle seine Ladung nur einige wenige Millisekunden beibehalten kann, muss DRAM kontinuierlich aufgefrischt werden, damit der Speicherinhalt erhalten bleibt.

Drosselung Die Fähigkeit einer CPU, Energie zu sparen und weniger Wärme zu erzeugen, indem sie bei geringer Auslastung oder bei drohender Überhitzung langsamer arbeitet. Intels Version dieser Technologie heißt *SpeedStep*, diejenige von AMD *PowerNow!*.

Druckauflösung Ein Maß für die Qualität der Druckerausgabe.

Drucker Ein Ausgabegerät, das Texte und Grafiken zu Papier bringt. Microsoft bezeichnet damit außerdem die Software, die den Drucker ansteuert.

Druckerwarteschlange Speichert Druckaufträge, die der Reihe nach von einem Drucker abgearbeitet werden.

Druckkopf Das Gehäuse, das bei einem Punktmatrixdrucker die Drucknadeln beherbergt.

Drucknadeln Die winzigen Nadeln, die bei einem Punktmatrixdrucker das Farbband gegen das Papier drücken, um Punkte zu erzeugen.

DSL (**Digital Subscriber Line**) Hochgeschwindigkeits-Internetverbindungen, die herkömmliche Telefonleitungen verwenden. DSL ist in asynchronen (ADSL) oder synchronen (SDSL) Varianten und mit verschiedenen Geschwindigkeiten verfügbar.

DTS (Digital Theatre System) Eine Technologie zur Rauschunterdrückung, die mit Dolby Digital vergleichbar ist.

Dual-Boot Bezeichnet einen Computer, auf dem zwei Betriebssysteme installiert sind, sodass der Benutzer beim Start auswählen kann, welches er laden möchte. Manchmal ist damit auch ein zweiter Neustart gemeint – falls der erste nicht richtig funktioniert hat.

Dual-Channel-Architektur Die gleichzeitige Nutzung zweier korrespondierender RAM-Module (RDRAM oder DDR SDRAM), um den Datendurchsatz zu erhöhen. Siehe auch *Triple-Channel-Architektur* und *Quad-Channel-Architektur*.

Dual-Channel-Arbeitsspeicher Eine Methode, die viele Mainboards nutzen, um schneller auf DDR-, DDR2- oder DDR3-RAM zugreifen zu können. Dazu sind jeweils zwei RAM-Module des gleichen Typs erforderlich.

Dumpster-Diving Das Durchsuchen von Abfällen nach Informationen.

Duplexeinheit Ein Mechanismus, der es Druckern ermöglicht, Papierblätter beidseitig zu bedrucken.

Duplexing Siehe *Disk-Duplexing*.

DVD (Digital Versatile Disc) Ein optisches Speichermedium, das 4 bis 17 GB Speicherplatz bietet.

DVD-ROM Das DVD-Pendant zur CD-ROM.

DVD-RW/DVD+RW Inkompatible wiederbeschreibbare DVD-Formate.

DVD-Video Ein speziell für digitale Videos ausgelegtes Format, das auf einer einzigen DVD Videomaterial hoher Qualität mit einer Länge von mehr als zwei Stunden speichern kann.

DVI (Digital Visual Interface) Ein digitaler Videoanschluss, den man vor allem bei PC-Grafikkarten und LCD-Bildschirmen findet. Einige Varianten unterstützen mittels eines speziellen Adapters auch analoge Videosignale.

`dxdiag` (DirectX Diagnostic Tool) Ein Diagnosewerkzeug, das Auskunft über die installierte DirectX-Version gibt.

Dynamische Datenträger Ein Windows-Feature, das es ermöglicht, dass sich ein einziges Volume über zwei oder mehr Laufwerke erstrecken kann. Dynamische Datenträger besitzen keine Partitionen, sondern Volumes. Sie können als gespiegelte Volumes, als Stripesetvolumes oder als gespiegelte Stripesetvolumes mit Parität verwendet werden.

ECC (Error Correction Code) Spezielle in Festplattenlaufwerken integrierte Software, die kontinuierlich nach defekten Sektoren sucht.

ECC RAM/DRAM (Error Correction Code DRAM) RAM-Bausteine mit speziellen Chips, die Speicherfehler aufspüren und beheben. Sie werden typischerweise in High-End-Servern eingesetzt, bei denen die Unversehrtheit der Daten eine große Rolle spielt.

Effektive Berechtigungen Die Berechtigungen eines Benutzers, die sich aus den kombinierten Berechtigungen durch die Mitgliedschaft in mehreren Gruppen ergeben.

EFS (Encrypting File System) Ein Dienst zur Organisierung und Verwaltung von Speicherplatz (wie z.B. NTFS), der in der Lage ist, die gespeicherten Daten zu verschlüsseln.

EIDE (Enhanced IDE) Ein Marketingkonzept des Festplattenherstellers Western Digital, das vier Verbesserungen des IDE-Standards umfasst: höhere Kapazitäten als 528 MB, vier gleichzeitig anschließbare Geräte, erhöhter Datendurchsatz sowie den Anschluss anderer Geräte als Festplatten. Siehe *ATAPI* und *PIO-Modus*.

Einadrige Leitung Ein Kabel, das zur Signalübertragung keinen hohlen Draht oder Litze verwendet, sondern einen einzelnen, soliden Draht.

Einbruchserkennung (Gehäuse) Ein Schalter in manchen Rechnergehäusen, der immer dann ausgelöst wird, wenn das Gehäuse geöffnet wird.

Einfache Dateifreigabe Ermöglicht die einfache Freigabe von Dateien, allerdings ohne Zugriffssteuerung auf Benutzerebene.

Einfaches Volume Ein Volume, das bei der Einrichtung eines dynamischen Datenträgers erstellt wird und sich wie eine primäre Partition verhält.

Ein-Faktor-Authentifizierung Ein weniger sicheres Authentifizierungsverfahren, bei dem nur ein Authentifizierungsfaktor erforderlich ist. Siehe *Mehrfaktor-Authentifizierung.*

Eingabeaufforderung Ein Programm zur Eingabe von Befehlen. Dem Benutzer wird durch die Eingabeaufforderung signalisiert, dass das Programm bereit ist, Eingaben entgegenzunehmen.

Eingabestift Ein Eingabegerät für die Stiftbedienung, das einem Kugelschreiber ähnelt.

Einseitig bestücktes RAM Ein RAM-Modul, das nur auf einer Seite der Platine mit RAM-Bausteinen bestückt ist.

Einstellungs-App Ein Tool in Windows 10, das eine große Anzahl ansonsten weit verstreuter und ungleichartiger Hilfsprogramme, Apps und Werkzeuge in einer halbwegs einheitlichen und praktischen App unter einen Hut bringt.

Elektrisches Potenzial Die Spannungsdifferenz zwischen zwei Objekten. Bei einem davon handelt es sich oft um Masse (Ground). Dieser Spannungsunterschied führt dazu, dass die Elektronen von einem Objekt zum anderen fließen möchten. Liegt eine erhebliche Potenzialdifferenz zwischen einer Person und beispielsweise einer Türklinke vor, kommt es beim Berühren zu einer Entladung in Form eines kleinen elektrischen Schlags. Siehe *Elektrostatische Entladung.*

Elektromagentische Interferenz (EMI) Durch elektromagnetische Interferenzen zwischen verschiedenen Geräten kann es zu Störungen kommen. So kommt es etwa zu einem verrauschten Bild, wenn Sie in unmittelbarer Nähe des Fernsehers einen Haartrockner einschalten. Ein weiteres Beispiel sind die »zittrigen« Bilder, die angezeigt werden, wenn Sie zwei Röhrenmonitore zu dicht nebeneinander stellen.

Elektromagnetischer Impuls (EMP) Ein potenziell schädlicher Puls elektromagnetischer Strahlung, der beispielsweise durch eine elektrostatische Entladung, Blitze, Detonation von Nuklearwaffen etc. verursacht wird.

E-Mail (Elektronische Mail) Eine Nachricht, für gewöhnlich Text, die eine Person per Computer einer anderen sendet. E-Mails können auch automatisch an eine Gruppe von Empfängern gesendet werden (Mailinglisten).

eMMC (Embedded MMC) Eine Flash-Speichertechnologie, die in vielen mobilen Geräten Einsatz findet.

Emulator Software oder Hardware, die Ein- und Ausgaben einer völlig anderen Plattform auf der Wirtsmaschine entgegennimmt bzw. darstellt.

Endbenutzer-Lizenzvereinbarung (EULA, End User License Agreement) Eine Vereinbarung, der Sie vor der Verwendung einer Software zustimmen müssen. Sie beschreibt die Nutzungsbedingungen und führt oft auch ausdrücklich auf, was dem Benutzer *nicht* erlaubt ist.

Entelektrisator Ein Gerät, das statische Aufladungen entfernt.

Entmagnetisierung Verhindert, dass unerwünschte elektromagnetische Felder in der Bildröhre entstehen, die zu verzerrter Darstellung und fehlerhaften Farben führen können. Dazu ist es erforderlich, elektrischen Strom durch eine Spule zu leiten. Die meisten Röhrenmonitore bieten eine Möglichkeit zur Entmagnetisierung (»Degaussing«).

Elektrostatische Entladung (ESD) Das unkontrollierte Abfließen der Elektronen von einem Objekt auf ein anderes. Elektrostatische Entladungen sind eine echte Bedrohung für PCs, da sie dauerhafte Schäden an Halbleiterbauteilen verursachen können.

Energieoptionen Ein Windows-Feature, das eine bessere Steuerung des Energieverbrauchs durch anpassbare Energiesparpläne wie AUSBALANCIERT, ENERGIESPARMODUS oder HÖCHSTLEISTUNG erlaubt.

Energiesparmodus Ein spezieller Modus, der die Funktionalität eines Geräts begrenzt oder ändert, um die Akkulaufzeit zu verlängern. Zu diesem Zweck werden beispielsweise WLAN und Mobilfunk deaktiviert, die Helligkeit des Bildschirms oder der Prozessortakt vermindert.

Ereignisanzeige Ein in Windows als MMC-Snap-In verfügbares Werkzeug, das es dem Benutzer ermöglicht, verschiedene Ereignisse zu überwachen oder die Auslastung von Netzwerk und CPU anzuzeigen.

Ereignisüberwachung Ein Feature der Ereignisanzeige im Bereich SICHERHEIT, das Protokolleinträge vornimmt, wenn bestimmte Ereignisse eintreten, z.B. wenn ein Benutzer sich anmeldet.

Erweiterte Startoptionen Ein Menü, das beim Systemstart aufgerufen werden kann und erweiterte Optionen anbietet, z.B. den Start im abgesicherten Modus oder die Aktivierung der letzten als funktionierend bekannten Konfiguration.

eSATA Ein auf dem Serial-ATA-Standard beruhender Anschluss für externe Festplatten und optische Laufwerke.

Eskalieren Wenn die beauftragte Person nicht in der Lage ist, ein Problem zu beheben, wird es eskaliert, z.B. indem ein Fachmann mit speziellen Kenntnissen hinzugezogen wird.

Ethernet Die von Xerox geprägte Bezeichnung des ersten Standards für Netzwerkverkabelung und -protokolle. Beruht auf einer Bus-Topologie.

Erweiterte Partition Eine nicht startfähige Partition der Festplatte. Pro Festplatte ist nur eine erweiterte Partition erlaubt. Ihr Zweck ist es, große Festplatten in kleinere Abschnitte mit jeweils eigenem Laufwerksbuchstaben zu unterteilen.

Erweiterungsbus Ein Satz von zur CPU führenden Leitungen, die durch den Erweiterungsbusquarz getaktet werden und direkt mit den verschiedenen Erweiterungssteckplätzen verbunden sind (PCI, AGP, PCIe usw.).

Erweiterungsbusquarz Steuert die Geschwindigkeit des Erweiterungsbusses.

Erweiterungssteckplätze Anschlüsse auf dem Mainboard, die es dem Benutzer erlauben, dem System zusätzliche Komponenten hinzuzufügen. Siehe auch *AGP*, *PCI* und *PCIe*.

exFAT Ein proprietäres Dateisystem von Microsoft, das Dateien mit einer Größe von mehr als 4 GB verwenden kann. Theoretisch werden 16 Exabyte (EB) große Dateien und eine Partitionsgröße von 64 Zettabyte (ZB) unterstützt. Es kommt vor allem bei Flash-Speichergeräten mit einer Kapazität von mehr als 2 TB zum Einsatz.

ExpressCard Die leistungsfähigere serielle Version der PC-Card, die im Laufe des letzten Jahrzehnts die PC-Card-Steckplätze in Laptops verdrängt hat. ExpressCards gibt es in zwei Varianten, die 34 oder 54 mm breit sind und als *ExpressCard/34* bzw. *ExpressCard/54* bezeichnet werden.

ext4 (Fourth Extended File System) Siehe *FAT64*.

Extensible Authentication Protocol (EAP) EAP-kompatible Anwendungen können auf eine Vielzahl unterschiedlicher Authentifizierungsmethoden zurückgreifen. Das Protokoll ist eigentlich für Authentifizierungen aller Art ausgelegt, wird allerdings fast ausschließlich in drahtlosen Netzwerken eingesetzt.

Externe Lautsprecher Tragbare Geräte, die den Klang von Smartphones, Tablets oder Laptops deutlich verbessern. Die Verbindung erfolgt meist über Bluetooth oder über den Kopfhöreranschluss.

Externer Datenbus (EDB) Die vorrangige Datenautobahn aller Computer. Alle Bestandteile Ihres Computers sind direkt oder indirekt mit dem externen Datenbus verbunden. Siehe auch *Frontside-Bus* und *Backside-Bus*.

Farbsublimationsdrucker Drucker, der eine wärmeempfindliche Rolle mit Kunststofffolie verwendet, in der Farbstoffe eingebettet sind, die durch Erhitzen in den gasförmigen Zustand übergehen und sich beim Abkühlen mit einem speziell beschichteten Papier verbinden. Auf diese Weise entstehen hochwertige Ausdrucke.

Farbtiefe Beschreibt die Fähigkeit eines Scanners, Farben, Farbtöne, Sättigung usw. wiederzugeben.

FAT (File Allocation Table) Versteckte Dateizuordnungstabelle, die aufzeichnet, wie die Dateien einer Festplatte in bestimmten Clustern gespeichert sind – für DOS die einzige Möglichkeit herauszufinden, wo sich der Inhalt einer Datei befindet. Der FAT-Eintrag des ersten Clusters einer Datei ist die Adresse des zweiten Clusters, der zum Speichern der Datei verwendet wird. Der FAT-Eintrag für den

zweiten Cluster ist die Adresse des dritten Clusters usw. Der Eintrag für den letzten Cluster schließlich ist ein spezieller Code, der das Dateiende kennzeichnet. Es gibt zwei identische FATs – für den Fall, dass eine davon zerstört oder beschädigt wird. Der Begriff bezeichnet auch die 16-Bit-FATs, die von Windows 2000 und anderen NT-basierten Betriebssystemen verwendet werden.

FAT32 Eine Dateizuordnungstabelle, die zur Adressierung und Indizierung der Cluster 32 Bit verwendet. Wird häufig für Flash-Speichermedien und Windows-Versionen vor XP eingesetzt.

FAT64 (exFAT) Ein proprietäres Dateisystem von Microsoft, das die Beschränkung der Dateigröße auf 4 GB aufhebt und Dateien mit einer Größe von bis zu 16 Exabyte (EB) unterstützt. Die maximale Größe einer Partition beträgt theoretisch 64 Zettabyte (ZB). Das Format wurde vornehmlich entwickelt, um Flash-Speichermedien mit Kapazitäten von mehr als 2 TB nutzen zu können.

`fdisk` Werkzeug zum Partitionieren von Festplatten (DOS und Windows 95).

Fehlerüberprüfung Ein grafisches Werkzeug in Windows, das Fehler auf Festplatten sucht und repariert. Häufig wird auch die Bezeichnung der ausführbaren Datei `chkdsk` (Check Disk) benutzt. Das Pendant in macOS heißt Festplattendienstprogramm und Linux bietet ein Kommandozeilenprogramm namens `fsck` an.

Festplattenlaufwerk Ein Speichergerät, bei dem schnell rotierende Platten aus einem magnetischen Material zum Lesen und Schreiben von Daten verwendet werden. Abkürzung HDD von engl. *Hard Disk Drive*.

Finder Der Dateibrowser in macOS.

Fingerabdruckscanner Ein biometrisches Gerät, das es ermöglicht, den Fingerabdruck einer Person zum Entsperren eines mobilen Geräts oder eines PCs einzusetzen.

Firewall Ein Gerät, das den Datenverkehr zwischen einem lokalen Netzwerk und dem Internet beschränkt.

FireWire (IEEE 1394) Ein Standard zur Übertragung von Breitbandsignalen über dünne serielle Leitungen. Dieser serielle Bus wurde von Apple und Texas Instruments entwickelt. Bis zu 63 Geräte können miteinander verbunden werden, und die maximale Datenübertragungsrate beträgt 800 Mbps. Wurde weitgehend von Thunderbolt abgelöst.

Firmware In ein Gerät integrierte Programme oder auf einem ROM-Chip gespeicherter Code. Die Firmware ist im Allgemeinen betriebssystemunabhängig und ermöglicht so ein breites Anwendungsspektrum ohne direkte Unterstützung durch ein Betriebssystem. Beim System-BIOS handelt es sich beispielsweise um Firmware.

Firmwareaktualisierung Ein Vorgang, bei dem das BIOS eines Mainboards aktualisiert wird, um Fehlerbehebungen und neue Funktionalitäten einzuspielen. Wird normalerweise mit dem CMOS-Setup-Programm durchgeführt, allerdings stellen manche Hersteller auch ein Windows-Programm zum Durchführen der Aktualisierung bereit.

Fitness-Armbänder Geräte, die zu körperlicher Ertüchtigung anregen sollen, indem sie mittels Beschleunigungssensoren Schritte zählen, die Pulsfrequenz messen, Laufstrecken aufzeichnen und den Benutzer durch Vibrationsalarme daran erinnern, sich in Bewegung zu setzen. Es gibt auch Geräte, die nicht wie eine Uhr am Handgelenk getragen, sondern mit einer Klammer an der Kleidung befestigt werden.

Fixiereinheit Ein Mechanismus in Laserdruckern, bei dem während des Druckvorgangs zwei Rollen den Toner auf dem Papier fixieren.

Flachbettscanner Der gebräuchlichste Scannertyp für Endkunden. Die Scanner-Beleuchtung bewegt sich beim Einscannen eines Bildes entlang des Flachbetts.

Flash-ROM Eine ROM-Technologie, die das Überschreiben der gespeicherten Daten erlaubt, während der Chip sich im PC befindet. Mit weitem Abstand das gebräuchlichste Speichermedium für das BIOS heutiger Computer, denn das Flash-ROM kann bei den meisten Systemen aktualisiert werden, ohne den Computer öffnen zu müssen.

FlexATX Ein ziemlich kleiner Formfaktor von Mainboards. Gemäß des FlexATX-Standards gefertigte Mainboards sind nochmals deutlich kleiner als microATX-Mainboards.

Flüchtiger Speicher Ein Speichertyp, der kontinuierlich mit Spannung versorgt werden muss, damit er seinen Inhalt beibehält.

Flugmodus Ein Modus von mobilen Geräten, in dem alle drahtlosen Netzwerke und der Mobilfunk deaktiviert sind und der beispielsweise beim Fliegen Einsatz findet.

Flüssigkeitskühlung Eine Kühlmethode, bei der eine Flüssigkeit (üblicherweise Wasser) durch einen Metallblock geleitet wird, der oben auf dem Prozessor aufsitzt und die Wärme absorbiert. Die Flüssigkeit wird vom Metallblock erwärmt, aus dem Block heraus in eine Kühlvorrichtung transportiert und dann wieder durch den Block gepumpt.

Flussumkehr Wenn eine magnetische Flussumkehr stattfindet, erkennt der Schreib/Lesekopf den Wechsel der magnetischen Polarität.

FM-Synthese Das Erzeugen von Klängen (Musik oder andere Soundeffekte) durch das Emulieren verschiedener Musikinstrumente.

`format` Kommandozeilenbefehl zum Formatieren eines Speichergeräts.

Formatieren Eine Partition für das Speichern von Daten vorbereiten, indem ein Stammverzeichnis und ein Dateisystem zur Organisation der Blöcke erstellt werden.

Formfaktor Ein Standard für den Aufbau der Komponenten auf dem Mainboard und dessen Größe. Die gebräuchlichsten Formfaktoren sind ATX, microATX und Mini-ITX.

FPU (Floating Point Unit) Formale Bezeichnung der Gleitkommaeinheit, dem mathematischen Coprozessor der CPU. Der Coprozessor führt Berechnungen in einem Fließkommazahlensystem aus (das Dezimalzahlen ermöglicht). Bevor der Intel 80486 auf den Markt kam, waren FPUs eigenständige Chips, nicht Bestandteil der CPU.

Fragmentierung Tritt auf, wenn durch das wiederholte Löschen und Neuanlegen von Dateien keine zusammenhängenden Bereiche zum Speichern von Daten verfügbar sind. Der Zugriff auf die Daten kann dadurch spürbar verlangsamt werden. Abhilfe schafft ein zu allen Windows-Versionen gehörendes Defragmentierungsprogramm. Siehe *Defragmentierung*.

Frame Eine über das Netzwerk übertragene Dateneinheit. Frames beinhalten mehrere Bestandteile, wie die MAC-Adressen des Absenders und des Empfängers, die eigentlichen Daten und die FCS (*Frame Check Sequence*).

Freeware Kostenlose Software, für die keine Lizenzgebühr entrichtet werden muss.

Freigegebene Dokumente Ein voreingestellter Windows-Ordner, auf den alle Benutzerkonten eines Systems zugreifen können.

Frequenz Ein Maß für die Tonhöhe (hoch oder tief).

Frequenzbandbreite Ein Teil des Spektrums, in dem die wichtigsten Frequenzanteile des übertragenen Signals liegen, beispielsweise eines Fernsehprogramms, einer Stimme oder Faxdaten. Das Signal benötigt bei der Übertragung einen bestimmten Frequenzbereich, der durch eine obere und untere Grenzfrequenz gekennzeichnet ist. Je größer die Bandbreite ist, desto schneller erfolgt die Übertragung. So wird es möglich, komplexere Signale (Audio, Video) zu übermitteln. Da die Bandbreite begrenzt ist, müssen andere Benutzer warten, wenn bereits eine Übertragung stattfindet.

Frontside-Bus Elektrische Leitungen, die CPU und Arbeitsspeicher des Systems miteinander verbinden. Der Frontside-Bus wird üblicherweise mit 66 bis 133 MHz getaktet und ist vom Backside-Bus und dem Erweiterungsbus zu unterscheiden (wenngleich es einige gemeinsame Leitungen mit Letzterem gibt).

FRU (Field Replaceable Unit) Alle Komponenten eines PCs, die sich beim Kunden vor Ort austauschen lassen. Eine offizielle Liste dieser Komponenten gibt es nicht. Ob ein bestimmtes Bauteil vor Ort ausgetauscht wird, hängt auch vom jeweiligen Reparaturdienst ab.

`fsck` Ein Kommandozeilenprogramm in Linux, das die Festplatte auf Fehler überprüft.

FTP (File Transport Protocol) Regeln, die es erlauben, dass zwei Computern während einer Dateiübertragung miteinander kommunizieren. Das Protokoll dient zur Datenübertragung über das Internet und verwendet die Portnummern 20 und 21.

Full-Speed-USB USB-Standard mit einer Datenübertragungsrate von 12 Mbps, der auch als USB 1.1 bezeichnet wird.

Funktionstaste (FN-Taste) Viele Laptops besitzen eine Sondertaste, die gedrückt gehalten werden muss, um bestimmten anderen Tasten eine zusätzliche Funktion zu verleihen.

Gain Siehe *Verstärkungsverhältnis.*

Gamepad Ein Eingabegerät, das speziell zum Steuern von Spielen gedacht ist. Gamepads besitzen für gewöhnlich zwei Steuerknüppel, eine Richtungssteuerung sowie eine Reihe weiterer verschiedener Tasten und Schalter.

Gastbenutzerkonto Ein stark eingeschränktes Windows-Benutzerkonto bzw. ein Mitglied der Gruppe GAST.

GDDR5 Die fünfte Generation DDR RAM, die vor allem von hochwertigen Grafikkarten verwendet wird.

GDI (Graphical Device Interface) Eine Windows-Komponente, die zur Verarbeitung eines Druckauftrags nicht den Drucker, sondern die CPU nutzt.

Gedruckte Schaltung Siehe *Leiterplatte.*

Gehäuselüfter Ein vom Mainboard geregelter Lüfter, der nicht direkt an der CPU angebracht ist.

Gemeinsam genutzter Speicher Eine Methode, um den auf der Grafikkarte erforderlichen Arbeitsspeicher zu reduzieren, indem sie das normale RAM des Systems nutzt. Senkt Kosten, verringert aber auch die Leistung.

Gemeinsame Nutzung der Internetverbindung Ein Windows-Feature, das es erlaubt, eine einzige Internetverbindung mehreren anderen Computern zur Verfügung zu stellen.

General Data Protection Regulation (GDPR) Siehe *Datenschutz-Grundverordnung.*

Geofencing Nutzung der Ortungsdienste eines mobilen Geräts, um zu erkennen, wenn es ein bestimmtes Gebiet erreicht oder verlässt.

Geotracking Eine Funktion von Mobiltelefonen, die es Mobilfunkanbietern und staatlichen Behörden ermöglicht, anhand der Identifizierungsnummer oder der MAC-Adresse jederzeit den Aufenthaltsort eines Geräts zu ermitteln.

Gepuffertes RAM Für gewöhnlich bei Mainboards anzutreffen, die mehr als vier Steckplätze für Speichermodule besitzen, weil es durch die zusätzlichen Module verstärkt zu Interferenzen kommen kann.

Geräte-Manager Ein Werkzeug, das es Technikern erlaubt, die Hardware und die Treiber eines Windows-PCs zu untersuchen und zu konfigurieren.

Geräte-Rack Eine Metallstruktur, die dazu dient, Netzwerk-Hardware sicher unterzubringen und Patchfelder zu montieren. Die Standardbreite eines Racks beträgt 19 Zoll. Das vertikale Ausmaß passender Geräte wird in Höheneinheiten (HE) angegeben.

Gerätetreiber Programme, die vom Betriebssystem zur Steuerung der Kommunikation zwischen dem Computer und Peripheriegeräten benutzt werden.

Gesichtserkennung Eine Technologie, die es ermöglicht, die Gesichtszüge einer Person zum Entsperren eines mobilen Geräts oder eines PCs einzusetzen.

Gespiegelte Laufwerke Gemäß RAID-Level-1 gespiegelte Volumes. Siehe *Spiegelung eines Volumes.*

Gesten Bestimmte Bewegungen, die ein Benutzer auf dem Touchscreen ausführt, wie beispielsweise Spreizen oder Zusammenkneifen der Finger, die für die verwendete App eine spezielle Bedeutung haben.

Giga Vorsilbe für 1.073.741.824 (2^{30}) oder für eine Milliarde. Ein Gigabyte entspricht 1.073.741.824 Byte – es sei denn, es geht um die Kennzeichnung der Speicherkapazität von Festplatten, denn hier bedeutet sie eine Milliarde. Ein Gigahertz entspricht einer Milliarde Hertz.

Glasfaserkabel Ein Kabel für Hochgeschwindigkeits-Datenübertragungen, das aus hochreinem Quarzglas oder Kunststoff (polymere optische Faser) besteht und von einer undurchsichtigen Hülle umgeben ist. Wird auch als Lichtwellenleiter (LWL) bezeichnet.

Gleichstrom Eine Form des elektrischen Stroms, die kreisförmig immer in dieselbe Richtung fließt (DC, *Direct Current*).

Goldene Regel Gehen Sie mit den Dingen anderer Menschen so um, wie Sie sich von anderen Menschen wünschen, dass sie Ihre Dinge behandeln.

Google Play Googles App- und Medien-Store für Android-Geräte.

GPS (Global Positioning System) Eine Technologie, die es mobilen Geräten ermöglicht, ihren genauen Standort zu bestimmen.

`gpresult` Kommandozeilenbefehl zur Anzeige der für einen Benutzer geltenden Gruppenrichtlinien.

GPU (Graphics Processing Unit) Ein spezialisierter Prozessor, der die CPU unterstützt, indem er die Berechnung von 3-D-Grafiken übernimmt.

`gpupdate` Kommandozeilenbefehl zur sofortigen Anwendung der Änderungen der Gruppenrichtlinien auf einem individuellen System.

Grafikkarte Steuert die Kommunikation zwischen CPU und Bildschirm.

Grafikmodus Eine bestimmte Kombination aus Auflösung und Farbtiefe.

Graustufentiefe Die Anzahl der Graustufen, die ein Scanner für jedes Pixel speichert.

`grep` Linux-Befehl zum Durchsuchen von Textdateien und Befehlsausgaben oder zum Herausfiltern überflüssiger Informationen.

Gruppe Eine Liste von Benutzerkonten mit denselben Berechtigungen.

Gruppenrichtlinie Eine Methode, Einstellungen für mehrere Netzwerk-Clients auf einfache Weise vorzunehmen, beispielsweise das Konfigurieren einer minimalen Kennwortlänge oder das Untersagen des Bearbeitens der Registry.

GSM (Global System for Mobile Communications) Ein Standard zur Datenübertragung per Funk für mobile Geräte.

GUI (Graphical User Interface) Eine grafische Benutzeroberfläche zur Interaktion mit dem Computer mittels Maus oder anderer Zeigegeräte, indem Symbole angeklickt oder bewegt werden, die Programme oder Dokumente repräsentieren, anstatt ausschließlich Texteingaben vorzunehmen.

GUID PT (Globally Unique Identifier Partition Table) Ein Partitionierungsschema, das mehr als vier Primärpartitionen erlaubt, ohne dynamische Datenträger zu verwenden.

Gyroskop Ein Gerät, das die Orientierung eines Smartphones oder Tablets im dreidimensionalen Raum ermitteln kann.

HAL (Hardware Abstraction Layer) Die Hardwareabstraktionsebene ist ein Teil des Windows-Betriebssystems, der systemspezifische Gerätetreiber vom übrigen Betriebssystem trennt.

Halb-Duplex Ein Übertragungsmodus, bei dem ein Gerät Daten entweder empfangen oder senden kann, aber nicht beides gleichzeitig.

Handshaking Ein Verfahren, das Modems, Terminals und Computer verwenden, um zu überprüfen, ob eine ordnungsgemäße Verbindung hergestellt werden konnte.

Hardware Physische Computerkomponenten, wie etwa elektrische, elektronische, magnetische oder mechanische Geräte. Sozusagen alles, was man anfassen kann. Eine Festplatte gehört zur Hardware, Microsoft Word hingegen nicht.

Hardware-Protokoll Legt viele Aspekte eines Netzwerks fest, angefangen bei Pakettypen bis hin zu den verwendeten Kabeln und Steckern oder Buchsen.

Hash Ein spezieller Wert, der anhand anderer Werte durch eine nicht umkehrbare Berechnung ermittelt wird. Für Hashwerte gibt es viele Anwendungsfälle, und sie spielen bei modernen Authentifizierungssystemen eine entscheidende Rolle. Statt die Benutzerkennwörter direkt in einer Datenbank zu speichern, die dann zu einem Angriffsziel für Hacker wird, speichert das Authentifizierungssystem lediglich den (*salted*) Hashwert eines Kennworts. Bei der Anmeldung wird der Hashwert anhand des angegebenen Kennworts erneut berechnet und mit dem vorhandenen Hash verglichen. Siehe auch *Salting*.

Hauptbenutzer Die zweitmächtigste Benutzergruppe in Windows nach der Gruppe Administratoren. Die Berechtigungen eines Hauptbenutzers unterscheiden sich in den verschiedenen Windows-Versionen allerdings etwas.

Hauptschlüssel Die Registry enthält fünf Hauptschlüssel:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_USERS
- HKEY_LOCAL_MACHINE
- HKEY_CURRENT_CONFIG

HBA (Host Bus Adapter) Verbindet SATA-Geräte mit dem Erweiterungsbus. Wird auch als SATA-Controller bezeichnet.

HDBaseT Ein kabelgebundenes Übertragungssystem für unkomprimierte hochauflösende Videos über Cat5a- oder Cat6-Netzwerkkabel.

HDD (Hard Disk Drive) Ein Speichergerät, bei dem schnell rotierende Platten aus einem magnetischen Material zum Lesen und Schreiben von Daten verwendet werden.

HDMI (High Definition Multimedia Interface) Ein Multimediaanschluss, über den sowohl hochauflösende Video- als auch Audiodaten übertragen werden. Dient zum Anschluss von LCD-Bildschirmen oder VR-Headsets am Computer.

HE (Höheneinheit) Eine Einheit zur Beschreibung von Geräte-Racks. Eine HE entspricht 1,75 Zoll bzw. 4,445 cm.

Heimnetzgruppe Eine Funktion von Windows 7 und neueren Windows-Versionen, die mehrere Computer miteinander verbindet, die dasselbe Kennwort verwenden – Benutzernamen sind nicht erforderlich. Ein Computer kann nur jeweils einer Heimnetzgruppe gleichzeitig zugehören. Heimnetzgruppen ermöglichen eine einfache Datei- und Druckerfreigabe in kleinen Netzwerken.

Heimnetzserver Ein Computer, der in einem kleinen Büronetzwerk oder in einem Heimnetzwerk seine Dienste anbietet.

Herstellereigener Store Ein Store, der Produkte nur eines Herstellers anbietet, wie z.B. der Apple Store.

Hex (Hexadezimal) Zahlensystem zur Basis 16, bei dem zehn Ziffern (0 bis 9) und sechs Buchstaben (A bis F) zur Notation verwendet werden. Binärzahlen lassen sich durch Hexadezimalzahlen sehr kompakt darstellen, indem jeweils vierstellige Binärzahlen durch eine einstellige Hexadezimalzahl ersetzt werden (die Hexadezimalzahl 9 entspricht z.B. der Binärzahl 1001).

Hierarchical File System Plus (HFS+) Klassisches Dateisystem älterer Macs, das für Time-Machine-Laufwerke noch immer erforderlich ist. In neueren Macs und kompatiblen älteren Systemen wird HFS+ durch APFS (Apple File System) ersetzt.

Hierarchischer Verzeichnisbaum Die Methode, die Windows zum Organisieren von Dateien in verschiedenen Ordnern unterhalb des Stammverzeichnisses verwendet. Siehe auch *Stammverzeichnis.*

High Dynamic Range (HDR) Eine Videotechnologie, die die Bandbreite und Intensität der Farbdarstellung über den Standardbereich hinaus vergrößert.

Highlevel-Formatierung Eine Formatierung, die ein Dateisystem auf einem Laufwerk einrichtet.

Hintergrundbeleuchtung Einer der drei wesentlichen Bestandteile eines LCD-Bildschirms, der zur Beleuchtung dient.

Hi-Speed USB USB-Standard mit einer Datenübertragungsrate von 480 Mbps, der auch als USB 2.0 bezeichnet wird.

Hochglanzbildschirm Ein Laptop-Bildschirm, der besseren Kontrast, sattere Farben und einen größeren Blickwinkel als ein matter Bildschirm bietet, allerdings auch stärker spiegelt.

Homescreen Der »Desktop« eines Smartphones oder Tablets.

Horizontalverkabelung Die Verkabelung, die Telekommunikations- oder Serverraum mit den Arbeitsplätzen verbindet.

Host (Netzwerk) Ein einzelnes Gerät in einem TCP/IP-Netzwerk, das eine IP-Adresse besitzt – jedes Gerät (normalerweise ein Computer), das Datenpakete senden und empfangen kann. In einer Umgebung mit Großrechnern beschreibt der Begriff einen zentralen Computer, auf den mehrere Benutzer gleichzeitig zugreifen.

Host (Virtualisierung) Geht es um Virtualisierung, bezeichnet der Ausdruck den Wirtsrechner, der mehrere virtuelle Betriebssysteme ausführt.

Host-ID Die Adresse eines TCP/IP-Geräts, wie beispielsweise Computer, Drucker, Kameras und so weiter.

`hostname` Kommandozeilenbefehl zur Anzeige des Namens eines Computers.

Hotspot Ein mit einem Mobilfunknetzwerk verbundenes mobiles Gerät, das von anderen Geräten als WLAN-Zugangspunkt verwendet werden kann. Es gibt zu diesem Zweck eigenständige Geräte, viele Smartphones und Tablets lassen sich aber ebenfalls als Hotspots verwenden.

Hot-swappable-Gerät Ein Gerät, das entfernt oder angeschlossen werden kann, ohne dass der laufende Betrieb des Systems unterbrochen werden muss.

HTML (Hypertext Markup Language) Textbasierte, Skript-ähnliche Auszeichnungssprache zum Erstellen von Hypertextdokumenten, wie sie im World Wide Web gang und gäbe sind.

HTPC Ein Heimkino-PC, an dem ein Fernseher oder ein Projektor angeschlossen ist, um damit Filme zu betrachten oder fernzusehen.

HTTP (Hypertext Transfer Protocol) Extrem schnelles Protokoll, das im WWW zum Übertragen von Dateien eingesetzt wird und den Port 80 verwendet.

HTTPS (HTTP over Secure Sockets Layer) Eine sichere HTTP-Variante, die im Internet für geschäftliche Transaktionen oder bei erhöhtem Sicherheitsbedarf genutzt wird. Sie verwendet Port 443.

Hub Ein in der Mitte eines Netzwerks mit Stern-Topologie befindliches elektronisches Gerät, an das alle Geräte im Netzwerk angeschlossen werden. Hubs übermitteln die Datenpakete überflüssigerweise an alle Ports und sind inzwischen von Switches verdrängt worden. Dennoch wird noch immer oft der Begriff »Hub« verwendet.

Hybrid Cloud Eine Kombination verschiedener Cloud-Typen, wie Public Cloud, Private Cloud und Community Cloud.

Hybrid-Gerät Ein tragbares Gerät, das die Leistung eines Laptops mit einem kleineren Formfaktor verbindet, z.B. ein Tablet.

Hybrid-Topologie Eine Netzwerk-Topologie, die Features mehrerer anderer Topologien kombiniert, wie z.B. die Stern-Bus-Topologie.

Hyperthreading Eine Prozessortechnologie von Intel, die es ermöglicht, dass eine Pipeline mehr als einen Thread gleichzeitig ausführt.

Hypervisor Eine Software, die es gestattet, auf einem einzelnen Computer mehrere Betriebssysteme gleichzeitig auszuführen.

I/O (Input/Output, Ein-/Ausgabe) Ein allgemeiner Ausdruck, der das Lesen und Schreiben von Daten bezeichnet. Eingaben können über die Tastatur und mit einem Zeigegerät wie einer Maus vorgenommen werden oder einer Datei entstammen. Ausgaben können auf dem Bildschirm erfolgen, in eine Datei geschrieben oder auf einem Drucker ausgegeben werden.

IaaS (Infrastructure as a Service) In der Cloud bereitgestellte virtuelle Server und Netzwerke.

iCloud Apples Cloud-Datenspeicher, der es Benutzern ermöglicht, alle Daten ihrer iPhones oder iPads in der Cloud zu sichern und von überall aus darauf zuzugreifen. Diese Daten umfassen neben den in iTunes erworbenen Mediendateien auch Kalender, Kontakte, Erinnerungen usw.

Icons Kleine Symbole oder Grafiken, die am häufigsten auf dem Desktop zu finden sind und geöffnet werden, wenn man sie doppelklickt.

IDE (Integrated Drive Electronics) Eine PC-Spezifikation für Festplattenlaufwerke kleiner bis mittlerer Größe, bei der die Steuerelektronik Teil des Laufwerks selbst ist, was die Datentransferrate erhöht und einen einfacheren Anschluss ermöglicht. IDE unterstützte nur zwei Laufwerke mit jeweils maximal 504 MB Speicherkapazität pro Anschluss und ist vollständig von EIDE verdrängt worden. EIDE unterstützt vier Laufwerke mit einer maximalen Speicherkapazität von jeweils rund 8 GB und ist mehr als doppelt so schnell. IDE ist die gebräuchlichere Bezeichnung für PATA-Laufwerke. Die Abkürzung wird mitunter auch als *Intelligent Drive Electronics* interpretiert. Siehe *PATA*.

Identifizieren des Problems Den Benutzer danach befragen, welche Änderungen kürzlich vorgenommen wurden oder was nicht mehr funktioniert. (Schritt 1 der CompTIA-Strategie zur Fehlersuche.)

IEEE (Institute of Electronic and Electrical Engineers) Ein weltweiter Berufsverband von Ingenieuren (vornehmlich aus den Bereichen Elektro- und Informationstechnik) mit Sitz in den Vereinigten Staaten, der Standards definiert.

IEEE 1394 Der IEEE-Standard für die Kommunikation über FireWire. Siehe *FireWire*.

IEEE 1394a FireWire-Standard für Datenübertragungen mit 400 Mbps.

IEEE 1394b FireWire-Standard für Datenübertragungen mit 800 Mbps.

IEEE 802.11 Standard für drahtloses Ethernet (WLAN).

`ifconfig` Linux-Befehl zur Anzeige von IP-Adressinformationen.

Image-Datei Eine bitweise Kopie von Daten, die auf CD oder DVD gebrannt werden sollen, die in einer einzigen Datei gespeichert sind. Bei den Daten kann es sich um einzelne Dateien oder komplette Laufwerke handeln. Besonders praktisch beim Kopieren von CD auf CD bzw. DVD auf DVD.

IMAP4 (Internet Message Access Protocol version 4) Eine Alternative zu POP3 zum Abrufen von auf einem Mailserver gespeicherten E-Mails. IMAP verwendet den TCP-Port 143.

IMC (Integrated Memory Controller) In die CPU eingebaute Schaltkreise, die einen schnelleren Zugriff auf Speicherbausteine ermöglichen, wie etwa den L3-Cache, der von mehreren Prozessorkernen gemeinsam genutzt wird.

IMEI (International Mobile Equipment Identity) Eine 15-stellige Nummer, die zur eindeutigen Identifizierung von mobilen Geräten dient, typischerweise Smartphones oder andere Geräte, die mit einem Mobilfunknetz verbunden sind.

Impedanz Ein Maß für den elektrischen Widerstand, den eine Leitung einem elektrischen Signal bietet, an dem erkennbar ist, für welche Datenübertragungsraten die Leitung geeignet ist.

IMSI (International Mobile Subscriber Identity) Eine eindeutige Nummer, die den Benutzer einer bestimmten SIM-Karte repräsentiert. Die IMSI kann beim Mobilfunkanbieter erfragt werden, um zu gewährleisten, dass ein gestohlenes Mobiltelefon nicht missbraucht wird. Die IMSI kann auch zum Entsperren eines Mobiltelefons verwendet werden.

Infobereich Enthält Icons von Hintergrundprozessen und zeigt die Uhrzeit sowie einen Lautstärkeregler an. Der Infobereich befindet sich standardmäßig am rechten Ende der Taskleiste.

Informationstechnologie (IT) Das Fachgebiet, das sich mit Computern, deren Betrieb und Wartung befasst.

Infrastruktur-Modus Ein Modus drahtloser Netzwerke, bei dem ein Zugangspunkt verwendet wird, um die drahtlosen Netzknoten mit einem Netzwerksegment zu verbinden.

Inkrementelles Backup Sichert alle Dateien, deren Archiv-Attribut aktiviert ist, das besagt, dass sie seit dem letzten Backup verändert worden sind. Nach erfolgter Sicherung wird das Archiv-Attribut deaktiviert.

Installations-Medium Typischerweise eine CD-ROM/DVD oder ein USB-Speicherstick, auf denen alle erforderlichen Treiber für ein Gerät gespeichert sind.

Integer Eine ganze Zahl. Integers und Fließkommazahlen werden von Programmen und von der CPU unterschiedlich gehandhabt.

Integrität Stets das Richtige tun.

Interferenzen Störungen, die durch Geräte ausgelöst werden, die elektromagnetische Strahlung aussenden, wie z.B. Mobiltelefone, drahtlose Netzwerkkarten oder Mikrowellenherde.

Interpolation Eine Technologie zur Aufzeichnung und Wiedergabe von Videos, die Farb- und Helligkeitswerte zwischen Pixeln näherungsweise berechnet, um nicht direkt aufgezeichnete Informationen zu ergänzen.

Interrupt Die Unterbrechung eines Prozesses, beispielsweise die Ausführung eines Programms, durch ein externes Ereignis, die so erfolgt, dass der Prozess später fortgesetzt werden kann. Zu solchen Ereignissen gehören beispielsweise Signale von Überwachungssensoren oder das Betätigen einer Unterbrechungstaste durch einen Benutzer.

Intrusion Detection System (IDS) Ein Programm, das Datenpakete inspiziert und nach aktiven Eindringlingen sucht. Ein IDS arbeitet im internen Netzwerk und kann Bedrohungen erkennen, die einer Firewall entgehen, wie etwa Viren, unberechtigte Anmeldeversuche und andere wohlbekannte Angriffsmethoden. Kann auch Bedrohungen aus dem internen Netzwerk erkennen, beispielsweise die Ausführung eines Schwachstellenscanners durch einen verärgerten Mitarbeiter.

Intrusion Prevention System (IPS) Hat große Ähnlichkeit mit einem IDS, mit dem Unterschied, dass der Datenverkehr direkt über das System läuft. Dadurch kann ein IPS einem laufenden Angriff selbst Einhalt gebieten. Allerdings kann der Datenverkehr dadurch auch verlangsamt werden. Zudem stellt es einen Single Point of Failure dar.

Inverter Ein Bauteil, das Gleichstrom in Wechselstrom umwandelt. Die Kaltkathodenlampen in Laptops und Flachbettscannern verwenden üblicherweise Inverter.

iOS Das Betriebssystem von Apples mobilen Geräten.

IP-Adresse Numerische Adresse eines mit einem Netzwerk wie dem Internet verbundenen Computers. Eine IPv4-Adresse besteht aus vier Oktetten von 8-Bit-Binärzahlen, die als Dezimalzahlen angegeben werden. Eine IPv6-Adresse ist 128 Bit lang. Die IP-Adresse kann in eine Netzwerk- und eine Host-ID unterteilt werden. Gelegentlich wird auch die Bezeichnung *Internetadresse* verwendet.

`ipconfig` Kommandozeilenbefehl für Windows-Rechner, der die aktuelle TCP/IP-Konfiguration anzeigt. Vergleichbar mit `ifconfig`.

IPS (In-plane Switching) Eine Anzeigetechnologie, die ältere TN-Panels (*Twisted Nematic*) abgelöst hat und kräftigere Farben sowie einen besseren Blickwinkel bietet.

IPsec (Internet Protocol security) Das von Microsoft eingesetzte Verschlüsselungsverfahren für mehrere über private Leitungen miteinander verbundene Netzwerke, das eine transparente Verschlüsselung der zwischen Server und Client ausgetauschten Daten bietet.

IPv4 (Internet Protocol version 4) Das Standard-Internetprotokoll, das auch ungleichartigen Netzwerken eine Verbindungsmöglichkeit bietet. Über dieses Protokoll werden Datenpakete zwischen Hosts ausgetauscht und gegebenenfalls über Gateways geleitet. Bestandteil des TCP/IP-Protokollstacks. IPv4-Adressen werden als vier durch Punkte voneinander getrennte Dezimalzahlen notiert: x.x.x.x. Dabei steht x jeweils für eine 8-Bit-Binärzahl mit einem Wert zwischen 0 und 255. Ein Beispiel: 192.168.4.1.

IPv6 (Internet Protocol version 6) Ein Protokoll, dessen Adressen aus acht Gruppen von jeweils vier Hexadezimalzahlen bestehen, deren Wert zwischen 0000 und FFFF liegt. Als Trennzeichen dient ein Doppelpunkt (»:«). Ein Beispiel: fedc:ba98:7654:3210:0800:200c:00cf:1234.

IrDA (Infrared Data Association) Ein Protokoll zur Kommunikation über Infrarotlicht, das Datenübertragungsraten von bis zu 4 Mbps erzielt.

IRQ (Interrupt Request) Ein Signal eines Geräts (z.B. Modem oder Maus), das anzeigt, dass es CPU-Rechenzeit benötigt. Bei PCs werden IRQs über bestimmte den verschiedenen Geräten zugewiesene IRQ-Kanäle übermittelt. Früher waren IRQ-Konflikte beim Hinzufügen von Erweiterungskarten an der Tagesordnung, aber dank der Plug&Play-Spezifikation bereiten solche Konflikte kaum noch Probleme.

ISA (Industry Standard Architecture) Der originale IBM PC besaß ISA-Steckplätze, über die zusätzliche Hardware an das Mainboard angeschlossen werden konnte. Für den AT-Computer entwickelte IBM einen 8-Bit-Erweiterungsbus mit einer Taktung von 8,33 MHz und veröffentlichte den Entwurf lizenzfrei. Später wurde eine verbesserte 16-Bit-Version ebenfalls lizenzfrei veröffentlicht. ISA-Steckplätze wurden Mitte der 1990er-Jahre von PCI verdrängt.

ISDN (Integrated Services Digital Network) Ein Standard der CCITT, der digitale Kommunikationsverfahren definiert, die herkömmliche analoge Telefonsysteme ersetzen sollen. ISDN ist normaler Sprachtelefonie überlegen, da es Transferraten von 128 Kbps beim Senden von Daten unterstützt. Außerdem können Leitungen gleichzeitig für Daten und Sprache genutzt werden. Durch DSL ist der Bedarf für ISDN stark zurückgegangen.

ISO-9660 Ein CD-Format, das PC-Dateisysteme auf CD-Medien unterstützt. Häufig wird auch die allgemeinere Bezeichnung CD File System (CDFS) gebraucht.

ISO-Datei Vollständige Kopie (Image) eines Speichermediums, das typischerweise für optische Medien verwendet wird. ISO-Image-Dateien tragen für gewöhnlich die Dateinamenendung `.iso`.

ISP (Internet Service Provider) Ein Unternehmen, das (normalerweise gegen Bezahlung) einen Internetzugang anbietet.

ITX Eine Reihe verschiedener Mainboard-Formfaktoren. Der gebräuchlichste und größte ITX-Formfaktor ist Mini-ITX, der aber dennoch ziemlich klein ist.

`iwconfig` Linux-Befehl zur Anzeige und zum Ändern der Einstellungen für das drahtlose Netzwerk.

Jailbreaking Die Umgehung der Einschränkungen auf einem iOS-Gerät.

Jokerzeichen Siehe *Wildcard*.

Joule Eine Maßeinheit für Energie, die in diesem Buch dazu dient, die zulässige Energiemenge anzugeben, die ein Überspannungsschutz verträgt, bevor er ausfällt.

Joystick Ein Peripheriegerät, das meist zum Steuern von Computerspielen verwendet wird, insbesondere für Flugsimulatoren. Ursprünglich war der Joystick als Allzweckeingabegerät konzipiert.

Jugendschutz Siehe *Kindersicherung*.

Jumper Zwei kleine Pins, die mit einer Steckbrücke kurzgeschlossen werden können, um bestimmte Einstellungen eines Computersystems zu konfigurieren, die sich nur selten ändern.

Kacheln Die Bausteine der Modern-UI-Benutzeroberfläche von Windows 8, bei denen es sich um potenziell »intelligente« Verknüpfungen handelt, die sich ändernde Informationen dynamisch anzeigen können, ohne dass die dazugehörige App geöffnet werden muss.

Kalibrierung Die Kalibrierung sorgt dafür, dass die auf dem Bildschirm angezeigten Farben mit denen eines Ausdrucks übereinstimmen.

Kaltgerätestecker Das PC-Netzteil wird über ein Kabel mit Kaltgerätestecker an einer Wandsteckdose angeschlossen.

Kaltkathodenlampe Eine Beleuchtungstechnologie, die in LCD-Bildschirmen und Flachbettscannern eingesetzt wird. Kaltkathodenlampen benötigen in Anbetracht der Lichtmenge, die sie liefern, vergleichsweise wenig Energie.

Kantenglättungsverfahren Siehe *Anti-Aliasing*.

Kapazitiver Touchscreen Ein Touchscreen, der auf die Potenzialdifferenz zwischen Bildschirm und Ihrem Körper reagiert, um die Bewegungen Ihrer Finger zu erkennen.

Kartenleser Ein Gerät, mit dem Sie auf Speicherkarten verschiedenen Typs zugreifen können.

Katastrophaler Ausfall Der Begriff beschreibt einen Ausfall, bei dem eine Komponente oder Teile des Systems so stark beeinträchtigt sind, dass das System als Ganzes nicht mehr startet. Oft ist ein vom Hersteller defekt ausgeliefertes Bauteil daran beteiligt. Ursache kann auch Überhitzung oder eine physische Beschädigung einer Komponente sein.

Kein Startlaufwerk erkannt Ein beim Startvorgang auftretender Fehler. Häufig wird er dadurch verursacht, dass ein nicht startfähiger USB-Stick angeschlossen ist oder noch irgendeine CD/DVD im optischen Laufwerk liegt.

Kennwort Eine Zeichenfolge, die zur Überprüfung der Identität eines Benutzers verwendet wird.

Kennwortrücksetzdatenträger Ein externes Speichermedium, z.B. eine Diskette oder ein USB-Stick, mit dem Benutzer ihr Kennwort zurücksetzen können, ohne den Zugriff auf verschlüsselte oder kennwortgeschützte Daten zu verlieren. Der Kennwortrücksetzdatenträger muss allerdings proaktiv vom Benutzer rechtzeitig erstellt werden, denn dazu ist die Eingabe des Kennworts erforderlich.

Kerberos Ein vom MIT entwickeltes verschlüsseltes Authentifizierungsverfahren, das sowohl aufseiten des Servers als auch clientseitig plattformunabhängig ist.

Kernel Im Arbeitsspeicher befindliche Programme, die für die wichtigsten Aufgaben des Betriebssystems zuständig sind.

Kernel Panic Das Linux-Pendant zu einem BSoD. Ein Fehler, der einen Neustart des Betriebssystems erforderlich macht. Siehe *BSoD*.

Keylogger Eine Software, normalerweise Malware, die die Eingaben auf einem Computer aufzeichnet und manchmal auch versendet, um an Kennwörter zu gelangen und Informationen über andere Aktivitäten des Benutzers zu sammeln, wie den Besuch von Webseiten.

`kill` In UNIX-Shells (wie Bash) und der PowerShell wird mit diesem Befehl der angegebene Prozess beendet.

Kindersicherung Werkzeuge zum Überwachen und Beschränken von Benutzeraktivitäten, die dazu gedacht sind, dass Eltern festlegen können, auf welche Inhalte ihre Kinder zugreifen dürfen.

Klangfarbe Die unterschiedlichen Merkmale bei der Wiedergabe derselben Note auf verschiedenen Instrumenten.

Knowledge Base Siehe *Wissensdatenbank*.

Koaxialkabel Ein Kabel mit zentralem Leiter, der von einem zweiten, parallel verlaufenden Leiter (der Abschirmung) umgeben ist.

Kommandozeile Eine Schnittstelle zum Betriebssystem, die ohne grafische Benutzeroberfläche auskommt.

Kompatibilitätsmodus Ein Windows-Feature, das es erlaubt, für ältere Windows-Versionen geschriebene Programme unter neueren Windows-Versionen auszuführen.

Komponentenausfall Tritt auf, wenn ein Bauteil aufgrund eines Produktionsfehlers oder aus einem anderen Grund nicht mehr funktioniert.

Komponentendienste Programmierwerkzeuge in Windows, die den Austausch von Datenobjekten zwischen verschiedenen Anwendungen erlauben.

Komprimierung Der Vorgang, die Größe von Dateien durch Eliminierung von Redundanzen zu verringern, damit sie weniger Speicherplatz belegen und schneller übertragen werden können.

Konformität Das Konzept, dass Mitglieder einer Organisation sich bestimmten Regeln unterwerfen müssen. Aus der Sicht des Technikers geht es dabei oft darum, welche Software auf den firmeneigenen Rechnern installiert werden darf.

Kontextmenü Ein kleines Menü, das angezeigt wird, wenn ein Objekt mit der rechten Maustaste angeklickt wird.

Koronadraht Ein in der Nähe der Belichtungstrommel eines Laserdruckers befindlicher Draht, an dem eine sehr hohe Spannung anliegt. Der Koronadraht erzeugt ein elektrisches Feld, das dafür sorgt, dass Ladungen auf die Belichtungstrommel fließen können, um die lichtempfindlichen Tonerpartikel auf deren Oberfläche negativ aufzuladen. Neuere Drucker verwenden hierfür eine *Ladewalze*. Siehe auch *Unterer Koronadraht*.

Kreditkartenleser Ein Gerät, das an einem Smartphone oder Tablet angeschlossen wird und die Entgegennahme von Zahlungen per Kreditkarte ermöglicht.

Kreuzschlitzschraubendreher Eines der wichtigsten Handwerkszeuge für PC-Techniker.

KVM-Umschalter (Keyboard, Video, Mouse) Ein Gerät, mit dem Sie mit nur einem Bildschirm, einer Tastatur und einer Maus mehrere Computer steuern und deren Ausgabe anzeigen können.

LAN (Local Area Network) Eine Gruppe über Kabel, Funk oder Infrarot miteinander verbundener Computer, die diese Verbindungen dazu nutzen, Ressourcen wie Drucker oder Massenspeicher gemeinsam zu nutzen.

Laptop Ein zusammenklappbarer, tragbarer Computer mit Bildschirm, Tastatur und Trackpad.

Laser Eine kohärente, monochromatische Lichtquelle, die irgendwelche Verrückte manchmal dazu benutzen, um Piloten von Verkehrsflugzeugen zu blenden.

Laserdrucker Ein elektrofotografischer Drucker, der einen Laser als Lichtquelle verwendet.

Latenzzeit Die Verzögerung, mit der ein Gerät auf eine Anfrage reagiert. Meistens geht es bei Latenzzeiten um die Geschwindigkeit von RAM-Modulen.

Laufwerksbuchstabe Ein Buchstabe zur Kennzeichnung einer bestimmten Festplatte oder Partition.

Laufwerksgeometrie Zahlenangaben, die drei Werte beschreiben: Anzahl der Köpfe, der Zylinder und der Sektoren pro Spur. Sie legen fest, wo die Festplatte Daten speichert.

launchd Ein Werkzeug, das macOS verwendet, um geplante Aufgaben automatisch auszuführen.

Launcher Eine Android-App, die als Desktop des Geräts dient und oft mehr Konfigurationsmöglichkeiten bietet als die Launcher, die Google oder der Gerätehersteller bereitstellen.

Lautsprecher Ein Gerät, das mittels einer durch magnetische Kräfte in Schwingungen versetzte Membran Töne wiedergibt.

LBA (Logical Block Addressing) Ein Adressierungsverfahren, das dem Betriebssystem die Speicherbereiche auf einem Speichergerät als eine Reihe von Blöcken präsentiert, die mit `LBA0` beginnt. Das erspart es dem Betriebssystem, sich selbst um die Organisation des Speicherplatzes auf einer Festplatte oder SSD kümmern zu müssen.

LCD (Liquid Crystal Display) Ein bei tragbaren Computern weitverbreiteter Bildschirmtyp, der inzwischen auch die für Desktop-PCs früher verwendeten Röhrenmonitore verdrängt hat. LCD-Bildschirme verwenden Flüssigkristalle und elektrische Felder zur Darstellung von Bildern.

LED (Light-emitting Diode) Ein Licht ausstrahlendes Halbleiter-Bauelement mit den elektrischen Eigenschaften einer Diode.

LED-Monitor Ein LCD-Monitor, der statt Kaltkathodenlampen LEDs zur Hintergrundbeleuchtung verwendet und dadurch ein besseres Kontrastverhältnis sowie eine bessere Bildqualität erzielt.

Leistung Eine Registerkarte im Task-Manager, die zur Anzeige der Systemleistung dient.

Leistungsaufnahme Ein Maß dafür, wie viel Volt und Ampere zum Betrieb eines bestimmten Geräts erforderlich sind. Die Einheit für die Leistung ist das Watt (W).

Leistungsindikator Wird bei der Leistungsüberwachung dazu verwendet, Daten über ein bestimmtes Objekt zu sammeln.

Leistungsinformationen und -tools Ein Applet, das Ihnen einen Eindruck davon vermittelt, wie sich Ihr Computer im Vergleich mit anderen Systemen schlägt.

Leistungsoptionen Ein Applet, mit dem Sie CPU, RAM und virtuellen Arbeitsspeicher konfigurieren können.

Leistungsprotokolle und Warnungen Ein Snap-In, das so ziemlich alles protokollieren kann, was auf einem System vor sich geht.

Leistungsüberwachung Windows-Werkzeug zur Überwachung der Computerleistung.

Leiterbahnen Schmale elektrisch leitende Verbindungen in oder auf einer Leiterplatte.

Leiterplatte Auf einem elektrisch nicht leitenden Material (meist sehr robuste mit Expoxidharz getränkte Glasfasermatten) aufgebrachte Leiterbahnen aus Kupfer.

Letzte als funktionierend bekannte Konfiguration Eine der erweiterten Startoptionen, mit der Sie auf eine vorhergehende Konfiguration Ihres Computers zurückgreifen können, um größere Probleme beim Start zu beheben.

Level-1-Cache (L1-Cache) Der erste RAM-Cache, auf den die CPU zugreift. Er enthält nur Codeabschnitte und Daten, die für die aktuell laufenden Threads unentbehrlich sind. Der L1-Cache ist stets der kleinste und schnellste Cache-Speicher der CPU.

Level-2-Cache (L2-Cache) Der zweite RAM-Cache, auf den die CPU zugreift. Er ist deutlich größer und zumeist langsamer als der L1-Cache. Auf ihn wird nur zugegriffen, wenn sich die gesuchten Daten nicht im L1-Cache befinden.

Level-3-Cache (L3-Cache) Der dritte RAM-Cache, auf den die CPU zugreift. Er ist erheblich größer und langsamer als L1- und L2-Cache. Auf ihn wird nur zugegriffen, wenn sich die gesuchten Daten weder im L1- noch im L2-Cache befinden.

LGA (Land Grid Array) Die Anordnung der Pins auf dem CPU-Sockel, die zu den entsprechenden Kontakten auf der Unterseite der CPU gehören.

Lichtwellenleiter (LWL) Siehe *Glasfaserkabel*.

Lightning Ein proprietärer Stecker von Apple, der auf beiden Seiten acht Kontakte besitzt. Beim Anschließen spielt die Ausrichtung des Steckers keine Rolle, denn es gibt keine Ober- oder Unterseite. Der Anschluss dient zur Datenübertragung und Stromversorgung.

Lightweight Directory Access Protocol (LDAP) Ein von vielen Betriebssystemen zum Zugriff auf Verzeichnisdienste verwendetes Protokoll.

Li-Ion-Akku (Lithium-Ionen-Akku) Ein in mobilen Geräten häufig eingesetzter Akkutyp. Li-Ion-Akkus leiden, anders als Nickel-Cadmium-Akkus, nicht unter dem Memory-Effekt und liefern länger Strom, da sie eine deutlich höhere Energiedichte pro Gewichtseinheit besitzen.

Linklokale Adresse Die IPv6-Adresse, die sich ein Computer beim Start selbst zuweist. Hierbei handelt es sich um das IPv6-Pendant zur IPv4-APIPA-Adresse.

Linux Ein quelloffenes, unixoides Betriebssystem.

Liquid Contact Indicator (LCI) Flüssigkeitskontaktindikatoren ändern dauerhaft ihre Farbe, wenn sie mit einer Flüssigkeit in Berührung gekommen sind, meist von Weiß nach Rot. Sie befinden sich an verschiedenen Stellen im Inneren von mobilen Geräten.

Lithium-Polymer-Akkus (LiPo-Akkus) Lithium-Polymer-Akkus sind technisch gesehen eine Variante von Li-Ion-Akkus, die einen festen Elektrolyten auf Polymerbasis verwenden. In der Praxis wird die Bezeichnung oft auch für in Polymerbeuteln verpackte herkömmliche Li-Ion-Akkus verwendet.

Live-DVD Die Windows-Installationsmedien, die eine Windows-Vorinstallationsumgebung (WinPE) direkt in den Arbeitsspeicher laden und nicht auf Festplatte oder SSD zugreifen.

LoJack Eine in manchen BIOS/UEFI-Versionen verfügbare Sicherheitsfunktion, die es ermöglicht, den Aufenthaltsort eines gestohlenen PCs zu ermitteln, Programme zum Aufzeichnen von Tastatureingaben zu installieren oder den gestohlenen PC aus der Ferne herunterzufahren.

Logische Laufwerke Formatierte Bereiche auf der erweiterten Partition einer Festplatte, denen (normalerweise) Laufwerksbuchstaben zugewiesen werden. Für den Benutzer sehen sie wie eigenständige Festplatten aus.

Lokale Benutzer und Gruppen Ein Werkzeug zur Verwaltung von Benutzerkonten und Gruppenmitgliedschaften.

Lokale Benutzerkonten Eine in einer verschlüsselten Datenbank gespeicherte Liste der Namen und Kennwörter der Benutzer, die auf ein System zugreifen dürfen.

Lokale Sicherheitsrichtlinie Ein Windows-Werkzeug zur Konfiguration einer lokalen Sicherheitsrichtlinie auf einem einzelnen PC.

Long Term Evolution (LTE) Der Mobilfunkstandard der vierten Generation, der (theoretisch) Up- und Downloadgeschwindigkeiten von 100 Mbps bzw. 1 Gbps erreicht. Er wird als echte 4G-Technologie vermarktet und wird auch als solche akzeptiert.

Loopback-Stecker Ein Gerät, das bei einem Loopback-Test zur Überprüfung der Buchse einer Netzwerkkarte verwendet wird.

Loopback-Test Ein Test, der prüft, ob eine Netzwerkkarte Daten senden und empfangen kann. Zu diesem Zweck wird ein Loopback-Stecker an der Netzwerkkarte angeschlossen.

Löschlampe Bauteil im Inneren eines Laserdruckers, das die Beschichtung der Belichtungstrommel durch Licht leitfähig macht.

Low-Speed-USB USB-Standard mit einer Datenübertragungsrate von 1,5 Mbps, der auch als USB 1.1 bezeichnet wird.

LPT-Anschluss Ein Anschluss, der auch als Druckeranschluss bezeichnet wird. Meistens ist damit der lokale Parallelanschluss gemeint.

LPX Der erste »schlanke« Formfaktor, der durch den NLX-Formfaktor abgelöst wurde.

`ls` UNIX-Pendant zum `dir`-Befehl, der den Inhalt eines Verzeichnisses ausgibt.

Lumen Maßeinheit für die Helligkeit eines Projektors oder einer anderen Lichtquelle.

LWL (Lichtwellenleiter) Siehe *Glasfaserkabel*.

M.2 Ein platzsparender Erweiterungssteckplatz in neueren Laptops, der früher als NGFF (*Next Generation Form Factor*) bezeichnet wurde. M.2 ist ein allgemeiner Erweiterungssteckplatz, der auch z.B. WLAN-Karten unterstützt. Er wird jedoch meist zur Installation einer NVMe-SSD verwendet.

Mac (oder Macintosh) Kurzbezeichnung für Apples Vorzeige-Betriebssystem, das auf Intel-basierter Hardware läuft. Die CompTIA bezeichnet das Betriebssystem als *Mac*. Apple selbst nennt das aktuelle Betriebssystem *macOS*.

MAC (Mandatory Access Control) Ein Autorisierungsverfahren mit obligatorischer Zugriffskontrolle, bei dem das System Zugriff auf Ressourcen anhand von Sicherheitskennungen und Freigabestufen gewährt. Es ist nicht so flexibel wie DAC (*Discretionary Access Control*, Zugriffskontrolle nach eigenem Ermessen), bei dem Benutzer Zugriffsrechte auf Ressourcen gewähren können, deren Eigentümer sie sind. MAC kommt in Organisationen zum Einsatz, die hohe Anforderungen an die Sicherheit stellen.

MAC-Adresse (Media Access Control) Eine eindeutige, allen Netzwerkkarten zugeordnete 48 Bit lange Adresse. Die IEEE weist den verschiedenen Herstellern Blöcke möglicher MAC-Adressen zu, um zu gewährleisten, dass die Adressen auch wirklich eindeutig sind. Die Sicherungsschicht (Schicht 2 im OSI-Schichtenmodell) verwendet die MAC-Adresse, um Rechner aufzuspüren.

MAC-Adressfilterung Eine Möglichkeit, den Zugriff auf drahtlose Netzwerke anhand der MAC-Adresse des drahtlosen Netzwerkadapters WLAN-fähiger Geräte zu beschränken.

macOS Ein Betriebssystem von Apple, das auf Desktops und Laptops läuft. Das auf UNIX beruhende macOS läuft, wie Microsoft Windows, auf Intel-basierter Hardware. Bis 2016 nannte Apple das Betriebssystem OS X. Siehe auch *Mac* und *OS X*.

Mailserver Ein vernetzter Rechner, der einen E-Mail-Dienst zur Verfügung stellt.

Mainboard Eine flache Platine im Inneren des Computergehäuses mit einer Vielzahl von Anschlüssen. Alle zu einem PC gehörenden Geräte und Komponenten sind direkt oder indirekt mit dem Mainboard verbunden, unter anderem CPU, RAM, Festplatten, optische Laufwerke, Tastatur, Maus und Grafikkarte.

Mainboard-Handbuch Eine wichtige Informationsquelle bei der Installation eines Mainboards. Hier finden Sie die verschiedenen Spezifikationen, z.B. welche CPUs und welche RAM-Typen verwendbar sind.

Man-in-the-middle-Angriff (MITM-Angriff) Ein Angreifer befindet sich zwischen zwei miteinander kommunizierenden Systemen, was ihm die Möglichkeit gibt, aus beiden Richtungen durchgehende Nachrichten zu beobachten, umzuleiten oder sogar zu verändern.

MAM (Mobile Application Management) Software, die es der IT-Abteilung eines Unternehmens ermöglicht, die Apps auf den mobilen Geräten der Angestellten zu verwalten.

Maschinensprache Binäre Instruktionen, die der Prozessor verstehen kann.

Massenspeicher Festplatten, SSDs, optische Laufwerke, USB-Speichersticks usw.

Matrixdrucker Siehe *Punktmatrixdrucker*.

Matter Bildschirm Ein Laptop-Bildschirm, der ein ausgewogenes Verhältnis zwischen kräftigen Farben und Spiegelungen bietet, in hellen Umgebungen aber sehr blass wirkt.

Maus Ein Eingabegerät, das der Benutzer zur Steuerung eines Zeigers auf dem Bildschirm verwendet, um Objekte auszuwählen.

MBR (Master Boot Record) Das BIOS übergibt beim Systemstart die Kontrolle an den hier gespeicherten Code.

MCC (Memory Controller Chip, dt. Speicher-Controller-Chip) Ein Chip, der die Anfragen der CPU nach Speicherinhalten verarbeitet. Früher handelte es sich tatsächlich um einen speziellen eigenständigen Chip, heutzutage ist diese Funktionalität zumeist in den Chipsatz oder im Prozessor selbst integriert.

MCH (**Memory Controller Hub**) Ein von Intel geprägter Begriff für das, was sonst als Northbridge bezeichnet wird.

`md (mkdir)` Kommandozeilenbefehl zum Erstellen von Ordnern.

MDM (**Mobile Device Management**) Die Verwaltung der verschiedenen mobilen Geräte, die zur Verarbeitung, Speicherung sowie zum Übermitteln bzw. Abrufen von Unternehmensdaten genutzt werden.

Medien-Streaming Das Versenden von Mediendaten, die auf Ihrem Computer unmittelbar wiedergegeben, aber nicht gespeichert werden.

Mega Vorsilbe für 1.048.576 (2^{20}) oder für eine Million. Ein Megabyte entspricht 1.048.576 Byte, ein Megahertz bedeutet hingegen eine Million Hertz.

Megapixel Ein Begriff, der vornehmlich zur Beschreibung der Leistungsfähigkeit von Digitalkameras verwendet wird.

Mehradrige Leitung Ein Kabel, das zur Signalübertragung mehrere feine Drähte (Litze) verwendet. Mehradrige Leitungen leiten den Strom zwar weniger gut als einadrige, vertragen aber eine beträchtliche Belastung, ohne zu brechen.

Mehrere Desktops Ein Feature der grafischen Benutzeroberfläche, das mehrere Desktops mit jeweils eigenem Hintergrundbild und Icons zur Verfügung stellt. macOS unterstützt mehrere Schreibtische mit *Spaces*. Die meisten Linux-Distributionen verwenden ebenfalls mehrere Desktops, die oft als »Workspaces« bezeichnet werden. Microsoft führte diese Funktion mit Windows 10 ein.

Mehrfaktor-Authentifizierung Ein Authentifizierungsverfahren, bei dem mehrere unabhängige Authentifizierungsfaktoren erforderlich sind, beispielsweise Kennwort und Fingerabdruck. Siehe auch *Ein-Faktor-Authentifizierung*.

Mehrkern-Verarbeitung Die vom Betriebssystem unabhängige Verteilung der Arbeitslast auf zwei oder mehr Prozessorkerne einer CPU.

Metro UI Die ursprüngliche Bezeichnung für die Benutzeroberfläche von Windows 8. Sie wurde aufgrund rechtlicher Bedenken in »Modern UI« umbenannt.

MFT (**Master File Table**) Die von NTFS verwendete, erweiterte Dateizuordnungstabelle. Siehe *FAT*.

MicroSD (**Micro Secure Digital**) Das kleinste Format von SD-Flash-Speicherkarten, das oft in Smartphones und Tablets zu finden ist.

Micro-USB Ein USB-Anschluss, den viele Android-Smartphones verwenden.

microATX (**µATX**) Eine Variante des ATX-Formfaktors, die das ATX-Netzteil verwendet. Die Mainboards sind im Allgemeinen etwas kleiner als ihre ATX-Pendants, besitzen aber die gleiche Funktionalität.

Microdrive Winzige Festplattenlaufwerke im CF-Kartenformat. Siehe auch *CompactFlash* (CF).

Microsoft Certified IT Professional (**MCITP**) Eine auf Microsoft-Produkte spezialisierte erweiterte Zertifizierung.

MIDI (**Musical Instruments Digital Interface**) Eine Schnittstelle, die Computer und elektronische Musikinstrumente verbindet. Statt umfangreicher Klangdaten übermittelt der Computer Anweisungen an das Instrument, die Angaben über Höhe, Klangfarbe und Dauer eines Tons enthalten. MIDI-Dateien sind daher äußerst effizient. Da eine MIDI-Datei keine digitalisierten Klangdaten enthält, sondern aus einer Reihe von Anweisungen besteht, kann sie leicht bearbeitet werden. Darüber hinaus ist es möglich, Töne über verschiedene Kanäle mehrstimmig wiederzugeben. Auf diese Weise kann ein ganzes Orchester simuliert werden.

MIDI-Geräte Externe Geräte, die es ermöglichen, Klanginformation im MIDI-Format einzugeben, beispielsweise ein MIDI-Keyboard (in Form einer Klaviatur).

Migration Der »Umzug« eines Benutzers und seiner Daten auf ein anderes Betriebssystem oder eine andere Festplatte.

Migrationstool für den Benutzerstatus Ein Programm für fortgeschrittene Anwender zum Übertragen von Dateien und Einstellungen mehrerer Benutzer.

Mikrofon Ein Eingabegerät zum Aufzeichnen von Audio.

Mikroprozessor Das »Gehirn« eines Computers und der wichtigste Chip, der die Geschwindigkeit und die Fähigkeiten eines Computers bestimmt. Eine andere Bezeichnung lautet CPU.

MIMO (Multiple In/Multiple Out) Ein Feature von Geräten nach dem IEEE-Standard 802.11n, das die gleichzeitige Nutzung von bis zu vier Antennen gestattet, wodurch der Datendurchsatz deutlich erhöht wird.

Mini-DIN Ein kleiner Stecker, der vornehmlich zum Anschließen von Tastaturen und Mäusen benutzt wird. Die meisten aktuellen Systeme verwenden statt des Mini-DIN-Steckers einen USB-Anschluss. Mini-DIN wird auch als PS/2 bezeichnet.

Mini-ITX Der größte und verbreitetste der drei ITX-Formfaktoren. Mit seiner Größe von nur 17 x 17 cm konkurriert Mini-ITX mit microATX und proprietären kleinen Formfaktoren.

Mini-(Molex-)Anschluss Ein Steckertyp von PC-Netzteilen, der Peripheriegeräte mit 5 und 12 Volt Spannung versorgt und auch unter der Bezeichnung »Floppy-Stecker« bekannt ist.

Mini-PCI Eine spezielle Form von PCI, die für die Verwendung in Laptops ausgelegt ist.

Mini-PCIe Eine spezielle Form von PCIe, die für die Verwendung in Laptops ausgelegt ist.

MiniSD (Mini Secure Digital) Das mittlere Format von SD-Flash-Speicherkarten.

Mini-USB Kleinerer USB-Anschluss, der oft bei Digitalkameras zu finden ist.

Mission Control Ein Feature von macOS, das es unter anderem erlaubt, zwischen geöffneten Anwendungen und Fenstern zu wechseln.

`mkdir` Siehe `md`.

MMC (Microsoft Management Console) Ein Shell-Programm in Windows, das verschiedene Hilfsprogramme, sogenannte Snap-Ins, zur Administration und Fehlerbehebung bereitstellt. Die MMC erlaubt es einem Administrator, die Verwaltungswerkzeuge an seine Bedürfnisse anzupassen, indem er diese aus einer Auswahl von Snap-Ins zusammenstellt, wie z.B. GERÄTE-MANAGER, BENUTZER UND GRUPPEN oder COMPUTERVERWALTUNG.

Mobilfunknetzwerke Netzwerke, die es Handys, Smartphones und anderen mobilen Geräten ermöglichen, sich mit dem Internet zu verbinden.

Modem (Modulator/Demodulator) Ein Gerät, das digitale Datenströme in ein analoges Signal konvertiert (Modulation) und eingehende analoge Signale wieder in digitale zurückverwandelt (Demodulation). Der analoge Kommunikationskanal ist für gewöhnlich eine Telefonleitung, und bei den analogen Signalen handelt es sich üblicherweise um Töne.

Molex-Anschluss Ein Steckertyp von PC-Netzteilen, der optische Laufwerke, Festplatten und Gehäuselüfter mit Spannung versorgt. Er ist so geformt, dass er nicht verkehrt herum eingesteckt werden kann.

Monitor Ein Gerät, das die Ausgaben eines PCs auf einer Bildröhre oder einem Flüssigkristallbildschirm (LCD) darstellt.

Mono Eine Audioaufnahme von nur einer Quelle (Mikrofon), im Gegensatz zu Stereoaufnahmen, die zwei Quellen verwenden.

`move` Kommandozeilenbefehl zum Verschieben einer Datei an einen anderen Speicherort.

MP3 Abkürzung für MPEG Audio Layer 3, einem Komprimierungsverfahren, das speziell dafür ausgelegt ist, Dateien, die hochwertige Audioaufnahmen enthalten, fast ohne Qualitätsverlust in sehr viel kleinere Dateien umzuwandeln.

MPEG-2 (Moving Pictures Expert Group) Der MPEG-Standard für Video- und Audiokomprimierung mit Auflösungen von bis zu 1.280 x 720 und 60 Bildern pro Sekunde.

MPEG-4 (Moving Pictures Expert Group) Der MPEG-Standard für Video- und Audiokomprimierung mit gegenüber MPEG-2 verbesserter Komprimierung.

`msconfig` (Systemkonfigurationsprogramm) Ausführbare Datei, die das Systemkonfigurationsprogramm startet, das es dem Benutzer in Windows 7 erlaubt, Autostart-Programme und wichtige Systemdateien zu konfigurieren. Diese Funktionalität wurde in Windows 8 in den Task-Manager verlagert.

MSDS (Material Safety Data Sheets) Sicherheitsdatenblätter, die über potenzielle Gefahren für die Umwelt und die richtige Entsorgung verschiedener Computerkomponenten Auskunft geben.

`msinfo32` Liefert Informationen über Hardware-Ressourcen, Komponenten und die Software-Umgebung. Wird auch als *Systeminformation* bezeichnet.

Multiboot-Installation Eine Betriebssysteminstallation, bei der auf einem einzelnen Rechner mehrere Betriebssysteme installiert werden.

Multifunktionsgerät Ein Gerät, das die Funktionen mehrerer Geräte bietet, wie etwa Drucker, Kopierer, Scanner und Faxgerät.

Multimeter Ein Gerät zum Messen von Spannung, Strom und Widerstand.

Multisession-Laufwerk Ein CD-Brenner, der auf einer einzigen beschreibbaren CD mehrere Sessions brennen kann. Solch ein Gerät kann die Sessions auch abschließen, sodass keine weiteren Spuren mehr geschrieben werden können.

Multitasking Die gleichzeitige Ausführung mehrerer Programme auf demselben Computer.

Multitouch Eine Eingabemethode vieler Smartphones und Tablets, die es gestattet, mehrere Finger zu verwenden, um bestimmte Aktionen auszuführen, beispielsweise mit zwei Fingern zu scrollen oder über den Bildschirm zu wischen, um zur nächsten Bildschirmseite zu wechseln.

Multiuser MIMO (MU-MIMO) Mit 802.11ac eingeführte neue MIMO-Version, die es einem WAP ermöglicht, an mehrere Benutzer gleichzeitig zu senden.

Musik-CD-R Eine beschreibbare CD mit einem speziellen Aufzeichnungsformat. Die Hersteller der Medien müssen eine pauschale Urheberrechtsabgabe bezahlen, um dem unerlaubten Vervielfältigen von Musik Rechnung zu tragen.

`mv` Der `move`-Befehl in Linux und macOS.

NAT (Network Address Translation) Das Übersetzen der IP-Adresse eines Systems in eine andere, bevor sie einem anderen, größeren Netzwerk übergeben wird. Zu diesem Zweck gibt es ein eigenes Programm, das auf einem System oder einem Router läuft. In einem NAT-Netzwerk wird den Systemen eine private IP-Adresse zugewiesen. Das System, auf dem die NAT-Software läuft, besitzt zwei Netzwerkanschlüsse. Einer ist mit dem privaten Netzwerk und der andere mit dem größeren Netzwerk verbunden.

Die NAT-Software nimmt die für das größere Netzwerk bestimmten Datenpakete der Client-Systeme entgegen und ersetzt die interne IP-Adresse durch seine eigene öffentliche IP-Adresse. Auf diese Weise können sich viele Rechner eine einzige IP-Adresse teilen.

Native Auflösung Die Auflösung eines LCD-Monitors, die der Anzahl der physisch vorhandenen Pixel des Bildschirms entspricht.

Native Command Queing (NCQ) Eine Optimierungsfunktion von SATA-Laufwerken, durch die höhere Lese- und Schreibgeschwindigkeiten erzielt werden.

Navigationsbereich Die Bezeichnung der Ordnerliste im Explorer von Windows 7.

`nbstat` Ein Kommandozeilenwerkzeug, das älter ist als Windows. Liefert NetBIOS-Informationen. Es ist zwar nicht mehr so nützlich wie früher, kann aber bei der Fehlersuche in kleinen Arbeitsgruppen helfen.

`net` Kommandozeilenbefehl in Windows, der Geräte im Netzwerk anzeigt, ohne dass es erforderlich ist, deren Namen zu kennen.

net use Dieser Befehl ermöglicht es, Netzwerkverbindungen herzustellen, zu trennen und Informationen über bestehende Verbindungen zu Netzwerkressourcen anzuzeigen.

`net user` Dieser Befehl ermöglicht es, Benutzerkonten anzulegen, zu löschen oder zu ändern.

NetBIOS (Network Basic Input/Output System) Ein Protokoll, das auf der Sitzungsebene des OSI-Schichtenmodells arbeitet. Dieses Protokoll öffnet und verwaltet Verbindungen anhand der Namen der beteiligten Computer. Es verwendet die TCP-Ports 137 und 139 sowie die UDP-Ports 137 und 138.

Netbook Ein kleiner, energiesparender Laptop, der hauptsächlich zum Surfen im Internet verwendet wird.

NetBoot Ein Werkzeug zur einfachen Installation, Aktualisierung und Verwaltung von macOS über das Netzwerk.

Network Attached Storage (NAS) Ein an das Netzwerk angeschlossenes Gerät, dessen einzige Aufgabe es ist, Dateien zu speichern und über das Netzwerk bereitzustellen.

Netzteil Versorgt den PC mit Strom, indem es die Wechselspannung aus der Steckdose in verschiedene niedrige Gleichspannungen umwandelt.

Netzteillüfter Ein kleiner Lüfter des Netzteils, der warme Luft aus dem Gehäuseinneren nach außen befördert.

Netzwerk Eine Schnittstelle im Windows-Explorer, die im Netzwerk vorhandene Geräte anzeigt, wie z.B. andere Computer oder Netzwerkdrucker.

Netzwerkdokumentation Ein Plan der Netzwerkkonfiguration einer Organisation und der Topologie dieses Netzwerk für Techniker, die das Netzwerk ändern oder reparieren müssen.

Netzwerkdrucker Ein direkt am Netzwerk angeschlossener Drucker.

Netzwerk-ID Eine Nummer, die das Netzwerk identifiziert, an das ein Gerät oder ein Computer angeschlossen ist. Eine solche Netzwerk-ID gibt es sowohl im TCP/IP-Protokollstack als auch in anderen Netzwerkprotokollen.

Netzwerkprotokoll Software, die eingehenden Datenverkehr von der Netzwerkkarte entgegennimmt und ihn an die Anwendungen weitergibt, für die er bestimmt ist. Von den Anwendungen nimmt sie ausgehenden Datenverkehr entgegen und leitet ihn an die Netzwerkkarte weiter, die ihn über das Netzwerk versendet.

Netzwerktechnologie Eine praktische Umsetzung einer Topologie und anderer wichtiger Standards, um eine Möglichkeit bereitzustellen, Daten über ein Netzwerk von einem Computer an einen anderen zu übertragen. Die verwendete Technologie legt eine Vielzahl der Aspekte eines Netzwerks fest, von der Topologie über die Art der Frames bis hin zu den verwendeten Kabeln und Steckern oder Buchsen.

Netzwerktopologie-Diagramm Ein Diagramm, in dem dargestellt ist, wie ein Netzwerk aufgebaut ist (inklusive Switches, Router, WAPs, Diensten und Arbeitsplatzrechnern).

Netzwerkverbindung Eine Methode, zwei oder mehr Computer miteinander zu verbinden. Siehe auch *Netzwerk*.

NFC (Near Field Communication) Eine Technologie, die eine drahtlose Kommunikation mobiler Geräte im Nahbereich ermöglicht, die mittlerweile für mobile Bezahldienste wie Apple Pay oder Google Pay eingesetzt wird.

NIC (Network Interface Card/Controller) Eine Erweiterungskarte oder eine Komponente des Mainboards, über die ein PC per Kabel an ein Netzwerk angeschlossen wird. Eine *drahtlose* NIC verwendet statt eines Kabels eine Funkverbindung.

Ni-Cd-Akku (Nickel-Cadmium-Akku) Ein Akkutyp, der in den ersten tragbaren Computern Verwendung fand. Nach heutigen Maßstäben waren Ni-Cd-Akkus schwer und ineffizient und litten außerdem unter dem sogenannten Memory-Effekt, der die Lebensdauer des Akkus drastisch verkürzen konnte. Siehe auch *Ni-MH-Akku* und *Li-Ion-Akku*.

Nichtflüchtiger Speicher Speicher, dessen Inhalt auch nach dem Ausschalten des Computers erhalten bleibt. Meist ist damit ein ROM- oder Flash-ROM-Chip gemeint, im weiteren Sinne zählen aber auch optische Medien, Festplatten und andere Speichergeräte dazu.

Ni-MH-Akku (Nickel-Metallhydrid-Akku) Ein Akkutyp, der in älteren tragbaren PCs eingesetzt wurde. Bei Ni-MH-Akkus bereitete der Memory-Effekt weniger Probleme als bei Ni-Cd-Akkus. Inzwischen wurden Ni-MH-Akkus durch Li-Ion-Akkus abgelöst. Siehe auch *Ni-Cd-Akku* und *Li-Ion-Akku*.

Nit Ein Maß für die Helligkeit von LCD-Bildschirmen. Typische LCD-Bildschirme haben etwa 100 bis 400 Nits.

NLQ (Near Letter Quality) Eine Bezeichnung für Punktmatrixdrucker, die einen Druckkopf mit 24 Nadeln besitzen.

NLX Der zweite »schlanke« Formfaktor, der den vorhergehenden LPX-Formfaktor ersetzte.

NMI (**Non-maskable Interrupt**) Ein nicht maskierbarer Interrupt, also eine Unterbrechung, die von der CPU nicht ignoriert werden kann, die typischerweise zu einem Blue Screen führt.

NNTP (**Network News Transfer Protocol**) Ein Protokoll, das Server verwenden, die Newsgroups anbieten.

Normales Backup Vollständiges Backup aller ausgewählten Dateien. Nach der Datensicherung wird das Archiv-Attribut deaktiviert.

Northbridge Ein Chip, der die CPU mit Arbeitsspeicher, PCI-Bus, Level-2-Cache und Grafikkarte verbindet und über den Frontside-Bus mit ihr kommuniziert. Bei neueren CPUs ist die Northbridge in die CPU integriert.

Notebook Siehe *Laptop*.

Notfalldiskette (**Emergency Repair Disk, ERD**) Speichert die unverzichtbaren Startdateien sowie Partitionsinformationen und ist bei älteren Windows-Versionen das wichtigste Werkzeug zum Beheben von Startproblemen. In neueren Windows-Versionen lautet die Bezeichnung »Systemreparaturdatenträger«.

`nslookup` Kommandozeilenprogramm in Windows, das die DNS-Informationen über einen angegebenen Hostnamen anzeigt.

NTFS (**New Technology File System**) Ein stabiles und sicheres Dateisystem, das Microsoft mit Windows NT eingeführt hat. NTFS bietet eine Vielzahl an Optionen hinsichtlich der Zugriffsberechtigungen und der Sicherheit. Benutzern kann der Zugriff auf einzelne Dateien gewährt werden. NTFS unterstützt lange Dateinamen, Komprimierung, Verschlüsselung und Berechtigungen auf Objektebene.

NTFS-Berechtigungen Legen fest, über welche Berechtigungen ein bestimmter Benutzer auf einem System verfügt, das NTFS verwendet.

Nutzungsrichtlinien Die Nutzungsrichtlinien legen fest, für welche Aufgaben Angestellte die firmeneigenen Geräte (Computer, Telefon, Drucker, Netzwerk) verwenden dürfen. Auch die Handhabung von Kennwörtern, E-Mail usw. sind darin geregelt.

NVIDIA Corporation Ein bedeutender Hersteller von Grafikkarten und Chipsätzen.

NVMe (**Non-Volatile Memory Express**) Eine SSD-Technologie, bei der die Kommunikation zwischen SSD und Betriebssystem direkt über eine PCI-Bus-Lane stattfindet. Dadurch sinkt die Latenzzeit und die Geschwindigkeit der hochwertigen SSDs wird vollständig ausgereizt. NVMe-SSDs gibt es in verschiedenen Bauformen, etwas als Erweiterungskarten, am gebräuchlichsten ist das M.2-Format. NVMe-SSDs sind derzeit noch deutlich teurer als andere SSDs, sie sind aber auch erheblich schneller. NVMe-Laufwerke verwenden SATAe.

NX-Bit Eine Technologie, die es der CPU erlaubt, bestimmte Speicherbereiche zu schützen. Die Funktion verhindert, zusammen mit einer Implementierung durch das Betriebssystem, Angriffe auf wichtige Betriebssystemdateien. Microsoft bezeichnet dieses Feature als Datenausführungsverhinderung (*Data Execution Prevention, DEP*), die standardmäßig aktiviert ist.

Objekt Eine Systemkomponente, der verschiedene Merkmale zugewiesen werden können und die vom Betriebssystem als eigenständiges Gebilde behandelt werden kann.

Objektzugriffsüberwachung Eine Funktion im Bereich SICHERHEIT der Ereignisanzeige, die Protokolleinträge vornimmt, wenn auf bestimmte Objekte zugegriffen wird, z.B. auf eine Datei oder einen Ordner.

ODBC-Datenquellen-Administrator Ein Werkzeug zur Konfiguration von ODBC-Datenquellen, das es ermöglicht, Datenquellennamen zu erstellen und zu verwalten, die auf Datenbanken verweisen. Die Datenquellennamen können von ODBC-fähigen Anwendungen genutzt werden, um über ODBC auf solche Datenbanken zuzugreifen.

Öffentlicher Ordner Ein allen Benutzern zugänglicher Ordner auf einem System oder im Netzwerk.

Offlinedateien Eine Funktion in Windows, die Kopien von Dateien und Ordnern auf einem Server auf der lokalen Festplatte speichert. Wenn ein Laptop mit dem Netzwerk verbunden wird, synchronisiert Windows diese Dateien automatisch mit denjenigen auf dem Server oder auf einem anderen PC.

Ohm Die Einheit für die Impedanz eines Kabels.

OLED (Organic Light-emitting Diode) Eine Anzeigetechnologie, bei der genau definierte Punkte in der Schicht einer organischen Verbindungen leuchten, daher benötigen OLEDs weder eine Hintergrundbeleuchtung noch einen Inverter. OLEDs kommen in hochwertigen Fernsehern oder in kleinen Geräten, wie Smartwatches, Smartphones oder VR-Headsets, zum Einsatz.

Open Source Der Begriff beschreibt Produkte, für die der Entwickler bzw. Hersteller Baupläne, Zusammensetzung und andere Informationen veröffentlicht. Er ist vor allem auf Software anwendbar.

Open-Source-Software Software, deren Quellcode nicht geheim gehalten wird, sondern öffentlich zugänglich ist. Die Software wird typischerweise unter einer Open-Source-Lizenz veröffentlicht, die Bedingungen für die Nutzung und Änderung des Codes festlegt.

OpenGL Eine der beiden gebräuchlichen APIs für Grafikkarten. OpenGL war ursprünglich für UNIX-Systeme entwickelt worden, wurde inzwischen aber auch auf Windows- und Apple-Systeme portiert. Siehe auch *DirectX*.

Optimierung An einem System vorgenommene Änderungen zur Verbesserung der Leistung.

Optionales ROM Eine alternative Methode, das Betriebssystem anzuweisen, wie mit einer Erweiterungskarte kommuniziert werden kann. Das Optionale ROM enthält ein BIOS für die Karte und ist in einem Chip auf der Karte selbst gespeichert.

Optische Auflösung Die von einem Scanner mechanisch erzielbare Auflösung. Die meisten Scanner setzen Software ein, um die Auflösung zu verbessern.

Optische Laufwerke Geräte zum Lesen und Beschreiben optischer Medien wie CDs und DVDs.

Optische Maus Ein Zeigegerät, das keine mechanischen Sensoren, sondern Licht verwendet, um festzustellen, in welche Richtung die Maus bewegt wird.

Optische Medien Verschiedene Datenträgertypen (wie CDs, DVDs, BDs usw.), die von einem Laser gelesen werden.

Originaleinstellung wiederherstellen Eine Option der Wiederherstellungsumgebung in Windows 8 und neueren Windows-Versionen, die das System vollständig zurücksetzt – alle Apps, Programme, Benutzerdaten und Benutzereinstellungen werden gelöscht. Nach der Auswahl dieser Option finden Sie ein frisch installiertes Windows vor. Sie sollten sie bei der Fehlerbehebung nur als allerletzten Ausweg benutzen. Und führen Sie vorher eine Datensicherung durch, falls möglich.

OS (Operating System/Betriebssystem) Programme und Code, die eine Benutzeroberfläche bilden, über die der Benutzer mit der Hardware des Systems interagieren kann, wie z.B. Windows, macOS und Linux.

OSI-Schichten-Modell Ein auf dem OSI-Protokollstack beruhendes Schichtenmodell, das den Datenfluss zwischen zwei Computern definiert und standardisiert. Im OSI-Modell gibt es die folgenden sieben Schichten:

- **Schicht 1: Bitübertragungsschicht** Legt die Form der Datenübertragung fest und wandelt Binärdaten in physikalische Impulse (elektronisch oder in Form von Licht) um. Auf der Bitübertragungsschicht arbeiten z.B. Repeater und Hubs.
- **Schicht 2: Sicherungsschicht** Identifiziert die Geräte der Bitübertragungsschicht, daher gehören MAC-Adressen zur Sicherungsschicht. Auf der Sicherungsschicht arbeiten z.B. Bridges.
- **Schicht 3: Vermittlungsschicht** Transportiert Datenpakete zwischen in verschiedenen Netzwerken befindlichen Computern. Auf der Vermittlungsschicht arbeiten neben Routern auch IP und IPX.
- **Schicht 4: Transportschicht** Splittet die Daten in kleinere Teile auf. TCP, UDP, SPX und NetBEUI arbeiten auf der Transportschicht.
- **Schicht 5: Sitzungsschicht** Verwaltet die Verbindungen zwischen den beteiligten Rechnern. Auf der Transportschicht arbeiten NetBIOS und Sockets.
- **Schicht 6: Darstellungsschicht** Kann auch verschlüsselte Daten handhaben; verbirgt die Unterschiede zwischen den verschiedenen beteiligten Computersystemen.
- **Schicht 7: Anwendungsschicht** Stellt den Anwendungen Werkzeuge zur Verfügung, um auf das Netzwerk (und die untergeordneten Schichten) zuzugreifen. HTTP, FTP, SMTP und POP3 sind Beispiele für Protokolle, die auf der Anwendungsschicht arbeiten.

OS X Das Betriebssystem für Apples ältere Macintosh-Computer, das auf einem UNIX-Kern beruht. Die ersten Versionen liefen auf Motorola-basierter Hardware (PowerPC), die neueren Versionen erfordert Intel-Hardware. Das »X« wird übrigens nicht wie der drittletzte Buchstabe des Alphabets ausgesprochen, sondern als »Zehn«. Wurde 2016 in *macOS* umbenannt.

P1-Stromanschluss Ursprünglich 20-poliger Stromanschluss für ATX-Mainboards; bei neueren Geräten 24-polig.

P4-Stromanschluss Stellt Mainboards, die den Pentium 4 und neuere Prozessoren unterstützen, zusätzliche 12 Volt für die CPU bereit.

PaaS (Platform as a Service) Cloud-basierte virtuelle Server und Werkzeuge zur Bereitstellung, Verwaltung und Wartung von Webanwendungen.

Paket Grundlegendes Element der Kommunikation über ein Netzwerk. Die Daten sind in Gruppen fester maximaler Größe aufgeteilt, die ein wohldefiniertes Format besitzen und als einzelne Objekte über das Netzwerk übertragen werden. Ein Paket enthält die Adressen des Absenders und des Empfängers sowie weitere Informationen, die zur Steuerung des Datenflusses dienen. Nicht zu verwechseln mit einem Frame, denn Pakete sind zwar Bestandteil eines Frames, aber nicht dasselbe.

PAN (Personal Area Network) Ein kleines drahtloses Netzwerk, das Computer per Bluetooth mit Peripheriegeräten verbindet.

Papierkorb Der Speicherort, an dem gelöschte Dateien abgelegt werden. Um Dateien wirklich endgültig zu löschen, muss der Papierkorb entleert werden.

Parallelanschluss Ein Anschluss zur synchronen Datenübertragung über parallele Leitungen an ein Peripheriegerät, für gewöhnlich ein sehr alter Drucker.

Parallele Ausführung Gleichzeitige Abarbeitung mehrerer Threads durch eine CPU mit mehreren Kernen.

Parität Eine Methode zur Fehlererkennung, bei der einer kleinen Gruppe übertragener Bits ein gerades oder ungerades Paritätsbit zugewiesen wird. Der Empfänger kann anhand des Paritätsbits feststellen, ob die übertragenen Daten gültig sind.

Paritätisches RAM Die erste Art von RAM mit Fehlererkennung, bei der ein zusätzliches Bit (das Paritätsbit) zur Überprüfung der Daten gespeichert wurde.

Partition Ein Abschnitt des Speicherbereichs einer Festplatte, der bei der Initialisierung erstellt werden muss, bevor sie formatiert werden kann.

Partitionierung Die Aufteilung einer physischen Festplatte in mehrere logische Abschnitte, die *Partitionen* oder *Volumes* genannt werden.

Partitions-Boot-Sektor Speichert für das Booten von der Partition erforderliche Informationen, wie den Speicherort der Bootdateien.

Partitionstabelle Eine im Bootsektor einer Festplatte gespeicherte Liste der Partitionen mit einem startfähigen Betriebssystem.

`passwd` Linux-Befehl zum Ändern des Benutzerkennworts.

Password Authentication Protocol (PAP) Die älteste und einfachste Form der Authentifizierung und auch die unsicherste, da alle Kennwörter im Klartext übermittelt werden.

PATA (Parallel ATA) Bei dieser Implementierung ist der Controller im Laufwerk selbst integriert. Siehe auch *ATA*, *IDE* und *SATA*.

Patch Eine kleinere vom Hersteller veröffentlichte Korrektur, die Fehler oder Probleme mit einer bestimmten Software behebt.

Patchfeld Ein Patchfeld enthält eine Reihe von Buchsen, die mit der Horizontalverkabelung verbunden sind. Patchfelder vereinfachen es, die Verkabelung zu organisieren und schützen die Horizontalverkabelung.

Patchkabel Kurze (typischerweise 50 bis 150 cm lange) UTP-Kabel, mit denen die Anschlüsse eines Patchfelds mit Switch oder Router verbunden werden.

PC auffrischen Eine Option der Wiederherstellungsumgebung in Windows 8 und neueren Windows-Versionen, die das Betriebssystem neu installiert, ohne Benutzerdaten (Dateien, Einstellungen) oder im Windows-Store erworbene Anwendungen zu löschen. Aber Achtung: Alle anderen Anwendungen auf Ihrem System werden beim Auffrischen gelöscht!

PCB (Printed Circuit Board) Siehe *Leiterplatte*.

PC-Card Kreditkartengroße Adapterkarten, die ältere Laptops und andere Geräte um bestimmte Funktionalitäten erweitern. Es gibt parallele 16-Bit- und CardBus-PC-Cards sowie serielle Express-Cards. Siehe *PCMCIA*.

PCI (Peripheral Component Interconnect) Eine Architektur für den Erweiterungsbus des Mainboards, die es ermöglicht, einem System weitere Komponenten hinzuzufügen. Sie verwendet den Local-Bus-Standard, was es über diesen Bus angeschlossenen Geräten erlaubt, die volle Geschwindigkeit des Mainboards (bis zu 33 MHz) zur Kommunikation mit der CPU zu nutzen, nicht nur die langsameren 8 MHz des normalen Busses. Die Daten werden, anders als beim älteren ISA-Standard, nicht als 8- oder 16-Bit-Blöcke übertragen, sondern als 32 oder 64 Bit große Pakete.

PCIe (PCI Express) Der serielle Nachfolger von PCI und AGP, der das Konzept individueller Datenpfade mitbringt, die sogenannten Lanes. Im Prinzip kann eine beliebige Anzahl von Lanes benutzt werden, aber eine einzelne Lane (x1) und 16 Lanes (x16) sind auf Mainboards am häufigsten zu finden.

PCIe-Stromstecker (6/8-polig) Ein Stecker an manchen PC-Netzteilen, der zur Stromversorgung einer eigenständigen Grafikkarte dient.

PCI-X (PCI Extended) Eine auf 64-Bit erweiterte PCI-Version, die typischerweise in Servern und High-End-Systemen zu finden ist.

PCL (Printer Command Language) Eine von Hewlett-Packard entwickelte Druckersprache, die auf einem breiten Spektrum von Druckern zum Einsatz kommt. In den Lernzielen der CompTIA ist von *Printer Control Language* die Rede.

PCM (Pulse Code Modulation) Ein in den 1960er-Jahren entwickeltes Tonformat zur Übertragung von Telefongesprächen über die ersten digitalen Leitungen.

PCMCIA (Personal Computer Memory Card International Association) Ein Konsortium von Computerherstellern, das den PC-Card-Standard entwickelt hat, eine kreditkartengroße Adapterkarte, die ältere Laptops und andere Geräte um bestimmte Funktionalität erweitert. PCMCIA wurde 2009 aufgelöst.

Pearson Vue Ein Unternehmen, das die CompTIA A+-Prüfungen verwaltet.

Peer-to-Peer-Modus Siehe *Ad-hoc-Modus*.

Peer-to-Peer-Netzwerk Ein Netzwerk, in dem jeder Rechner sowohl die Rolle des Clients als auch die des Servers einnehmen kann.

Pentium Die Bezeichnung der fünften und nachfolgender Generationen von Intel-Mikroprozessoren. Der erste Pentium besaß einen 32-Bit-Adressbus, einen 64 Bit breiten externen Datenbus und zwei Pipelines. Die weiteren Generationen tragen die Namen Pentium Pro, Pentium II, Pentium III und Pentium 4. Heutzutage bezeichnet Pentium die Einsteigermodelle in Intels Prozessorsortiment.

Peripheriegerät Ein an das System angeschlossenes Gerät.

Personal Digital Assistant (PDA) Eins der ersten mobilen Geräte. Mobilfunkverbindungen und Touchscreens gab es noch nicht, aber die Geräte beherrschten die grundlegenden Funktionen (Kontakte, Kalender usw.) heutiger Geräte.

Pfad Die genaue Angabe des Speicherorts einer Datei, inklusive der übergeordneten Verzeichnisse.

PGA (Pin Grid Array) Eine Prozessorbauform, bei der sich auf der Unterseite der CPU eine Vielzahl von Pins befindet. Es gibt viele verschiedene PGA-Varianten.

Phishing Der Versuch, Leuten Benutzername und Kennwort oder andere Zugangsdaten zu entlocken, indem man sich auf elektronischem Wege als jemand anderes ausgibt.

Pin 1 Eine Markierung, die gewährleisten soll, dass Stecker und Anschluss einer Festplatten korrekt ausgerichtet sind.

Piepcodes Eine Reihe akustischer Signale, die ein Mainboard beim POST von sich gibt. Diese Signale zeigen an, ob der POST erfolgreich war oder ob Teile der Hardware des Systems nicht korrekt funktionieren. Die Bedeutung der verschiedenen Tonsignale können Sie dem Handbuch des Mainboards entnehmen.

Piepser Siehe *Tonsonde.*

`ping` Kommandozeilenprogramm, das eine kleine Nachricht (ICMP ECHO) versendet, um zu überprüfen, ob ein anderer Computer mit dem Netzwerk verbunden ist, um potenzielle DNS-Probleme aufzuspüren, um Schwierigkeiten mit der Latenzzeit zu erkennen und so weiter.

Pinwheel of Death Eine sich drehende, regenbogenfarbige kleine Scheibe, die in macOS anzeigt, dass ein Programm nicht mehr reagiert.

Pipe Kommandozeilen-Operator, der das Zeichen »|« verwendet, um die Ausgabe eines Befehls einem anderen Befehl als Eingabe bereitzustellen, anstatt sie auf dem Bildschirm auszugeben.

Pipeline Ein Verarbeitungsverfahren zum gleichzeitigen Ausführen mehrerer Berechnungen, indem sie in eine Reihe einzelner Schritte aufgeteilt werden. Wird von vielen CPUs und GPUs verwendet.

Pixel (Picture Element) Das kleinste Element einer Computergrafik, dem eine Farbe oder eine Intensität zugewiesen werden kann.

PKI (Public Key Infrastructure) Ein Authentifizierungsverfahren, bei dem alle Beteiligten öffentliche Schlüssel in Form digitaler Zertifikate austauschen, um eine sichere Kommunikation über allgemein zugängliche Netzwerke wie das Internet zu gewährleisten.

Plan zur Lösung des Problems erstellen und umsetzen Nach dem Aufstellen und Überprüfen einer Theorie für die Ursache eines Fehlers, wird er vom Techniker behoben. (Schritt 4 der CompTIA-Strategie zur Fehlersuche.)

Platzhalterzeichen Siehe *Wildcard.*

Play Store Siehe *Google Play.*

Point-to-Point Tunneling Protocol (PPTP) Erweiterte Version des Point-to-Point-Protocol (PPP, wird für Einwahlverbindungen genutzt) mit verbesserter VPN-Unterstützung.

Plug-and-Play (PnP) Eine Kombination aus PC, Gerät und Betriebssystem, die bei der Installation eines neuen Peripheriegeräts dafür sorgt, dass alle Systemressourcen und Anschlüsse ordnungsgemäß konfiguriert werden.

Polygone Vielecke, die bei der Berechnung dreidimensionaler Grafiken von Objekten verwendet werden. Die Grafikkarte zeichnet eine Unmenge von Dreiecken und setzt sie zu Polygonen zusammen.

Polymorphes Virus Ein Virus, das versucht seine Signatur zu ändern, damit es von Antivirenprogrammen nicht erkannt wird.

POP3 (Post Office Protocol 3) Eins der beiden Protokolle, mit denen E-Mail von SMTP-Servern abgerufen werden kann. POP3 verwendet den TCP-Port 110. Früher verwendeten die meisten E-Mail-Clients POP3, aber inzwischen kommt das E-Mail-Protokoll IMAP4 häufiger zum Einsatz.

Pop-ups Störende Browserfenster, die beim Besuch einer Website automatisch erscheinen.

Port Eine Nummer, die beim Verbindungsaufbau zu einem TCP/IP-Host den angefragten Dienst (wie z.B. SMTP oder FTP) identifiziert. Einige Beispiele: 80 (HTTP), 443 (HTTPS), 21 (FTP), 23 (Telnet), 25 (SMTP), 110 (POP3), 143 (IMAP) und 3389 (RDP).

Portweiterleitung Verhindert die Übermittlung von IP-Datenpaketen auf anderen Ports als denjenigen, die der Systemadministrator dafür vorgesehen hat.

Port-Replikator Ein Gerät, das über einen USB-Anschluss oder einen anderen speziellen Anschluss mit dem Computer verbunden wird und weitere Anschlüsse zur Verfügung stellt, beispielsweise VGA, HDMI, USB, Ethernet und so weiter. Durch das Anschließen an einen Port-Replikator kann ein Laptop auf einen Schlag mit verschiedenen stationären Geräten wie Drucker, Scanner, Monitor oder einer Tastatur normaler Größe verbunden werden. Wenn zu Hause oder im Büro ein Port-Replikator eingesetzt wird, ist er für gewöhnlich bereits fest mit den stationären Geräten verbunden.

Positionierungsarm Der Mechanismus zum Bewegen der Schreib/Leseköpfe im Inneren einer Festplatte.

Positionsdaten Die GPS-Daten eines mobilen Geräts, die für Kartierungszwecke und für aufenthaltsortsabhängige Dienste genutzt werden, um beispielsweise in der Nähe befindliche Restaurants anzuzeigen oder Einkaufsgutscheine in umliegenden Geschäften einzulösen.

POST (Power-on Self Test) Grundlegende Diagnoseroutinen, die ein System zu Beginn des Startvorgangs ausführt, um zu gewährleisten, dass Grafikkarte und RAM installiert sind. Dann wird nach einem Betriebssystem gesucht. Wird eines entdeckt, erhält das Betriebssystem die Kontrolle über den Rechner.

POST-Karte Einfache Steckkarte, die in einen Erweiterungssteckplatz des Systems installiert wird und über eine kleine zweistellige LED-Anzeige verfügt, die darüber informiert, bei welchem Gerät ein Problem aufgetreten ist.

PostScript Von Adobe Systems entwickelte Seitenbeschreibungssprache. Die Seitenbeschreibung ist unabhängig von der Auflösung des Geräts, das zur Ausgabe benutzt wird. PostScript enthält außerdem eine Technologie zur Darstellung skalierbarer Schriften und kann Rasterbilder in vielen verschiedenen Größen und Auflösungen erzeugen.

Power-Good-Leitung Über diese Leitung wird die CPU aktiviert, nachdem festgestellt wurde, dass das Netzteil die richtige Spannung liefert.

Power over Ethernet (PoE) Eine Technologie, die Daten und Strom über ein einziges Ethernet-Kabel leitet.

PowerShell Siehe *Windows PowerShell*.

PPM (Pages per Minute) Die Geschwindigkeit eines Druckers (Seiten pro Minute).

PPP (Point-to-Point-Protocol) Ermöglicht es einem Computer, sich über eine Telefonwählverbindung mit dem Internet zu verbinden und die Vorteile einer direkten Verbindung zu nutzen.

Preboot Execution Environment (PXE) Eine Technologie, die es ermöglicht, einen PC ohne lokales Massenspeichergerät zu starten, indem das Betriebssystem über das Netzwerk von einem Server geladen wird.

Pretty Good Privacy (PGP) Ein Standard zum Senden und Empfangen verschlüsselter E-Mails. Siehe *Verschlüsselung*.

Primäre Partition Eine Partition auf einer Windows-Festplatte, auf der ein startfähiges Betriebssystem gespeichert werden kann.

PRL (Preferred Roaming List) Eine Liste der bevorzugten Anbieter beim Roaming, die gelegentlich von Ihrem Anbieter automatisch in der Firmware aktualisiert wird, damit Iihr Gerät mit den Frequenzen der verschiedenen Anbieter in der bevorzugten Reihenfolge konfiguriert ist, wenn es keine Verbindung zum Netzwerk Ihres Internetanbieters herstellen kann.

Problemberichte Ein Applet der Systemsteuerung, das Windows-Fehlerberichte anzeigt und weitere Informationen liefert, wie z.B. den Status der Firewall oder der Anti-Malware-Software.

Produktschlüssel (Product Key) Ein Code, der bei der Installation eingegeben wird, der die Rechtmäßigkeit der Software bestätigt.

Profil (Benutzer) Ein Benutzerprofil beschreibt die Voreinstellungen der Windows-Umgebung, wie Bildschirmhintergrund, Farben, Verknüpfungen und so weiter.

Profil (Farbe) Eine Liste verschiedener Einstellungen, die bei der Kalibrierung eines Bildschirms oder eines Druckers von einem Kalibrierungsgerät erstellt wird.

Profil (MDM) Konfigurationen und Sicherheitseinstellungen für das Mobile Device Management (MDM), die ein Administrator erstellt hat, um sie auf bestimmte Benutzergruppen oder Gerätekategorien anzuwenden.

Profil (Netzwerk) Die zur automatischen Verbindung mit einem WLAN erforderlichen Informationen, die unter der SSID des Netzwerks gespeichert werden.

Programm Eine Reihe von Anweisungen und Befehlen, die der CPU übermittelt werden, um Aufgaben zu erledigen.

Programme und Features Ein Applet, mit dem Programme manuell hinzugefügt oder entfernt werden können.

Projektionsdistanz Ein Maß für die Größe des projizierten Bildes bei einem bestimmten Abstand von Projektor und Projektionsfläche.

Projektor Oft auch Beamer genannt. Projiziert den Bildschirminhalt eines PCs oder andere Videoquellen auf eine Projektionsfläche, für gewöhnlich, um sie einem Publikum zu präsentieren.

Propagieren von Berechtigungen Beschreibt, wie die Berechtigungen beim Kopieren oder Verschieben von Dateien gehandhabt werden.

Proprietär Eine herstellerspezifische Technologie.

Proprietärer Absturzbildschirm Ein betriebssystemabhängiger Bildschirm, der einen NMI anzeigt. Siehe *NMI*.

Protokoll Eine Vereinbarung, auf welche Art und Weise der Informationsaustausch zwischen kommunizierenden Geräten stattfindet. Dazu gehört beispielsweise, wie viele und wie oft Daten gesendet werden, wie bei Übertragungsfehlern zu verfahren ist und wer die Daten empfängt.

Proxyserver Software, die es ermöglicht, mehrere Internetverbindungen über einen geschützten Rechner zu leiten. In Unternehmungsumgebungen sind Proxyserver eine gängige Sicherheitsmaßnahme. Anwendungen, die auf Ressourcen im Internet zugreifen möchten, fragen diese beim Proxyserver an, anstatt direkt auf das Internet zuzugreifen. Das schützt die Client-Computer und erlaubt es dem Netzwerkadministrator, den Internetzugriff zu überwachen und zu beschränken.

Prozesse Eine Registerkarte im Task-Manager, auf der alle laufenden Prozesse des Systems angezeigt werden. Oftmals nützlich, um nicht mehr reagierende Prozesse zu beenden.

ps Linux-Befehl zur Anzeige aller auf einem Computer laufenden Prozesse.

Punchdown-Tool Ein spezielles Werkzeug, mit dem die Drähte eines UTP-Kabels an einem Anschluss eines Patchfelds befestigt werden.

Punktmatrixdrucker Ein Druckertyp, bei dem die einzelnen Zeichen aus einem Punktmuster zusammengesetzt werden. Dabei drücken die Nadeln des Druckkopfs ein Farbband gegen das Papier, um Punkte zu erzeugen.

PVC (Polyvinylchlorid) Ein Material, das für die Ummantelung von Netzwerkkabeln verwendet wird, das bei einem Brand giftigen Rauch erzeugt.

pwd Linux-Befehl zur Ausgabe des aktuellen Arbeitsverzeichnisses.

Qi Standard für das drahtlose Aufladen.

QR-Scanner Ein Gerät zum Einlesen von QR-Codes.

Quad-Channel-Architektur Vergleichbar mit der Dual-Channel-Architektur, allerdings sind vier statt zwei RAM-Module erforderlich.

Quality of Service (QoS) Ein Router-Feature, das bevorzugten Zugriff auf Netzwerkressourcen ermöglicht. Dadurch wird gewährleistet, dass bestimmte Benutzer, Anwendungen oder Dienste Vorrang haben, wenn nicht genügend Bandbreite zur Verfügung steht, indem die Bandbreite anhand des Anwendungsprotokolls, der IP-Adresse oder anderer Merkmale begrenzt wird.

RAID (Redundant Array of Independent/Inexpensive Disks) Eine Methode zur Einrichtung fehlertoleranter Speichersysteme. Dabei werden mehrere Laufwerke in verschiedenen Konfigurationen miteinander kombiniert, die unterschiedliche Anforderungen an die Geschwindigkeit und die Redundanz erfüllen:

- **RAID 0** Striping auf Byteebene, das keine Fehlertoleranz bietet.
- **RAID 1** Spiegelung oder Duplexing mit Fehlertoleranz.
- **RAID 5** Striping auf Blockebene mit Parität. Erfordert mindestens drei Laufwerke.
- **RAID 6** Striping mit zusätzlicher Parität. Wie RAID 5, jedoch mit zusätzlichen Paritätsdaten. Erfordert mindestens fünf Laufwerke, von denen allerdings zwei ausfallen können, ohne dass es zu Datenverlust kommt.

- **RAID 0+1** Ein RAID 0, das aus zwei RAID 1 besteht. RAID 0+1 ist sowohl schnell als auch fehlertolerant, erfordert jedoch mindestens vier Laufwerke.
- **RAID 10** Die Umkehrung von RAID 0+1; ein RAID 1, das aus zwei RAID 0 besteht. RAID 10 ist ebenfalls schnell und fehlertolerant, erfordert jedoch auch mindestens vier Laufwerke.

Rainbow Table Eine komprimierte Datei, die Hashwerte von Kennwörtern (oder andere Zugangsdaten) und das dazugehörige Kennwort im Klartext enthält. Rainbow Tables dienen dazu, unsaltet Hashwerte älterer Authentifizierungssysteme in Kennwörter umzuwandeln, sind bei aktuellen Authentifizierungssystemen, die saltet Hashwerte verwenden, aber nutzlos.

RAM (Random Access Memory) Speicher mit wahlfreiem Zugriff, der gelesen und beschrieben werden kann, ohne dass die vorhergehenden Speicheradressen gelesen werden müssen. Für gewöhnlich ist damit der Hauptarbeitsspeicher eines PCs gemeint.

Ransomware Eine hinterhältige Art von Schadsoftware, die Daten und Laufwerke eines infizierten Systems verschlüsselt und für den Schlüssel zum Entschlüsseln Lösegeld fordert, oft mit einer zeitlichen Befristung.

Rapid Elasticity Die Möglichkeit, beim Cloud-Computing die Kapazität schnell zu erhöhen oder zu verringern. Da Cloud-Server auf virtuellen Maschinen laufen, können die Kunden nach Bedarf VMs beenden oder starten oder sie auf leistungsstärkere Hardware verschieben.

Raspberry Pi Ein besonders kleines, ARM-basiertes Mainboard, das viele Betriebssysteme und Peripheriegeräte unterstützt.

Rasterbild Ein Punktmuster, das eine Computergrafik darstellt.

Raumklang Verschiedene Befehle einer Soundkarte zum Erzeugen von Raumklang. Der Benutzer gewinnt dadurch den Eindruck, dass sich die Schallquelle vor, hinter oder seitlich von ihm befindet.

`rd (rmdir)` Kommandozeilenbefehl zum Löschen von Verzeichnissen.

RDP (Remote Desktop Protocol) Das von Remotedesktop verwendete Protokoll, das den TCP-Port 3389 nutzt.

ReadyBoost Ein Windows-Feature, das es erlaubt, Flash-Speichermedien als virtuellen Arbeitsspeicher zu nutzen.

Reaktionszeit Die Zeit, die es dauert, bis alle Subpixel eines LCD-Bildschirms von einem Zustand in einen anderen und wieder zurück wechseln.

Rechenvorgang Die vier Schritte, die bei Rechenoperationen erfolgen: Eingabe, Verarbeitung, Ausgabe und Speichern.

`regedit.exe` Ein Programm zur Bearbeitung der Registry.

Register Ein Speicherbereich in der CPU, der von den Schaltkreisen für Berechnungen verwendet wird. CPUs verfügen über eine Vielzahl von Registern, um verschiedene Funktionen ausführen zu können.

Registriertes RAM Siehe *Gepuffertes RAM.*

Registrierung Ein normalerweise optionaler Vorgang, bei dem sich der rechtmäßige Besitzer/Benutzer eines Produkts dem Hersteller gegenüber identifiziert.

Registry Eine komplexe Binärdatei, in der die Konfigurationsdaten eines Windows-Systems gespeichert sind. Zum Bearbeiten der Registry können Sie die Applets in der Systemsteuerung oder das Programm `regedit.exe` verwenden.

Remotedesktop Ein Windows-Werkzeug, das es ermöglicht, entfernte Rechner mit einer grafischen Oberfläche fernzusteuern.

Remoteinstallation Ein gängiges Verfahren zur Betriebssysteminstallation, bei dem sich die Installationsdateien in einem freigegebenen Verzeichnis auf einem Server im Netzwerk befinden. Der Rechner wird gestartet, mit dem Server verbunden und schon kann die Installation gestartet werden.

Remoteunterstützung Ein Windows-Feature, das es einem Benutzer ermöglicht, seinen Rechner von jemand anderem über das Internet fernsteuern zu lassen.

`ren (rename)` Kommandozeilenbefehl zum Umbenennen von Dateien und Ordnern.

Resistiver Touchscreen Ein Touchscreen, der auf Druck reagiert, der auf den Bildschirm ausgeübt wird.

Respektvoll Wie alle PC-Techniker ihre Kunden behandeln sollten.

Ressourcen Auf einem PC verfügbare Daten und Dienste, wie Dateien, Ordner, Laufwerke, Drucker, Netzwerkverbindungen und so weiter.

Ressourcenmonitor Ein Hilfsprogramm in Windows, das detaillierte Informationen über die Leistung der CPU, den Arbeitsspeicher, die Laufwerke und die Netzwerkaktivität anzeigt.

Ressourcenüberprüfungsprogramm Siehe *SFC*.

RET (Resolution Enhancement Technology) Siehe *Anti-Aliasing*.

RFI (Radio Frequency Interference) Siehe *Interferenzen*.

RG-6 Ein Koaxialkabel mit einer Impedanz von 75 Ohm, das beim Kabelfernsehen eingesetzt wird und Typ-F-Stecker verwendet.

RG-59 Ein Koaxialkabel, das für 10Base2-Netzwerke verwendet wird.

RIP (Raster Image Processor) Bestandteil eines Druckers, der Rasterbilder in Druckbefehle umwandelt.

Riser-Karte Eine spezielle Adapterkarte, die für gewöhnlich in einen eigenen Steckplatz auf dem Mainboard eingesetzt wird und die Ausrichtung der Erweiterungskarten relativ zum Mainboard ändert. Riser-Karten werden vor allem in kleinen, schlanken Gehäusen eingesetzt, um Tiefe und Höhe des Systems gering zu halten. Wird manchmal auch als »Tochterboard« bezeichnet.

Risikoanalyse Eine ausführliche Beurteilung der Probleme, die eine Änderung mit sich bringen könnte.

RJ-Anschluss (Registered Jack Connector) Ein Anschluss für UTP-Kabel, der für Telefonie- und Netzwerkverbindungen eingesetzt wird. Der RJ-11-Stecker besitzt vier Kontakte und wird üblicherweise zum Anschluss von Telefonleitungen benutzt. Der RJ-45-Stecker verfügt über acht Kontakte und dient normalerweise zum Anschließen von UTP-Netzwerkkabeln.

`rm` Linux-Befehl zum Löschen von Dateien.

`rmdir` Siehe *`rd (rmdir)`*.

Roaming Die Verbindung eines mobilen Geräts mit einem Netzwerk, das nicht seinem Mobilfunkanbieter gehört.

`robocopy` Leistungsfähiges Kommandozeilenprogramm zum Kopieren von Dateien und Ordnern, auch über das Netzwerk.

ROM (Read-Only Memory) Allgemeine Bezeichnung für nichtflüchtigen Speicher, der zwar lesbar, aber nicht beschreibbar ist. Im ROM gespeicherte Programme und Daten können also nicht versehentlich gelöscht werden. Außerdem bleiben die gespeicherten Daten auch nach dem Ausschalten erhalten, daher ist ROM perfekt dazu geeignet, ein BIOS oder Informationen wie naturwissenschaftliche Konstanten zu speichern.

Rooten Die Umgehung der Einschränkungen auf einem Android-Gerät, um Zugriff auf das Root-Benutzerkonto zu erlangen.

Rootkit Ein Programm, das sich grundlegende Funktionen des Betriebssystems zunutze macht, um Root-Rechte zu erlangen und sich vor Anti-Malware-Software zu verstecken, was auch gelingt, wenn nicht außerordentlich aggressive und spezialisierte Anti-Malware eingesetzt wird. Davon können Betriebssystem, Hypervisor und sogar Firmware betroffen sein.

Router Ein Gerät, das verschiedene Netzwerke miteinander verbindet. Datenpakete werden anhand der Netzwerkadresse des verwendeten Protokolls von einem Netzwerk in ein anderes weitergeleitet. Beispielsweise entscheidet ein IP-Router anhand der Netzwerk-ID, wohin er ein Paket weiterleitet. Router arbeiten auf Schicht 3 (Vermittlungsschicht) des OSI-Modells.

RS-232 Von der EIA (*Electronics Industry Association*) empfohlener Standardanschluss für serielle Geräte.

RSA-Token Erzeugt Zufallszahlen, die zusammen mit Benutzernamen und Kennwort für erhöhte Sicherheit sorgen.

Ruhezustand Eine Einstellung in den Energieoptionen, die dafür sorgt, dass alle im RAM befindlichen Daten auf die Festplatte geschrieben werden, bevor das System in den Ruhezustand versetzt wird. Beim Beenden des Ruhezustands werden die Daten wieder in den Arbeitsspeicher eingelesen.

SaaS (Software as a Service) Ein Cloud-basierter Dienst zum Speichern, Verteilen und Aktualisieren von Programmen und Anwendungen. Das SaaS-Modell ermöglicht überall, wo eine Internetverbindung verfügbar ist, den Zugang zu allen benötigten Anwendungen, ohne dass weitere Daten mitgeführt werden müssten oder regelmäßige Programmaktualisierungen erforderlich sind. Im Unternehmensumfeld erleichtert das Abo-Modell der SaaS-Anbieter die Finanzplanung und Hunderte oder Tausende von Rechnern greifen stets auf die aktuellste Software zu.

Salting Eine Schutzmaßnahme, die verhindern soll, dass aus Hashwerten mithilfe von Rainbow Tables Kennwörter im Klartext abgeleitet werden. Den Kennwörtern werden weitere Werte hinzugefügt, bevor der Hashwert berechnet und gespeichert wird.

Sampling Das Aufzeichnen von Klängen in einem elektronischen Format.

SAS (Serial Attached SCSI) Ein schneller und stabiler Speicher, der auf dem SCSI-Befehlssatz beruht. Unterstützt auch SATA-Laufwerke. Wird vorwiegend für Server und Speicherarrays verwendet.

SATA (Serial ATA) Die serielle Version des ATA-Standards, die gegenüber PATA (Parallel ATA) viele Vorteile aufweist, beispielsweise dünnere Kabel, verpolungsgeschützte Stecker und geringeren Energieverbrauch.

SATA 3.2 Eine weitere Bezeichnung für SATAe. Siehe SATA Express.

SATA Express (SATAe) Eine SATA-Version, die kompatible Laufwerke direkt an den PCI-Express-Bus des Mainboards anbindet. Jede PCIe-3.0-Lane erreicht einen Datendurchsatz von 8 Gbps. Ein SATAe-Laufwerk, das zwei Lanes nutzt, erzielt somit einen Datendurchsatz von satten 16 Gbps über den Bus.

SATA-Stromanschluss Ein 15-poliger, L-förmiger Stecker, den SATA-Laufwerke verwenden, die im laufenden Betrieb entfernt bzw. angeschlossen werden können.

Satelliten-Latenz Kleine Verzögerungen, die durch die Laufzeit der Signale über die zurückzulegende Distanz verursacht werden.

Satelliten Zwei oder mehr Stereolautsprecher, die zusammen mit einem Subwoofer ein Soundsystem bilden (z.B. 2.1, 5.1, 7.1 usw.).

Scalable Link Interface (SLI) Eine Technologie zum Anschließen von zwei oder mehr NVIDIA-Grafikkarten an einem einzelnen System. AMD hält mit der CrossFire-Technologie dagegen.

Scancode Ein allen Tasten einer Tastatur zugeordneter eindeutiger Code, den der Tastatur-Controller beim Betätigen einer Taste an die CPU übermittelt.

Schlüsselbundverwaltung Der Dienst zum Verwalten von Kennwörtern in macOS, der neben Kennwörtern auch Schlüssel und Zertifikate für Computer, Webseiten usw. speichert.

Schneller Benutzerwechsel Eine nützliche Option, wenn mehrere Benutzer ein System gemeinsam verwenden. Andere Benutzer können sich anmelden, ohne dass der aktuelle Benutzer sich abmelden muss.

Schnellstart-Symbolleiste Ermöglicht das Starten häufig verwendeter Programme mit einem einzigen Klick.

Schreibgeschützt-Attribut Ein Dateiattribut, das verhindert, dass eine Datei geändert wird. Nützlich, um Systemdateien zu schützen, die nicht bearbeitet werden sollten.

Schrittmotor Eine der beiden Methoden, den Positionierungsarm eines Festplattenlaufwerks zu bewegen. Siehe auch *Schwingspulenmotor*.

Schutzbrille Sorgt dafür, dass Ihre Augen geschützt sind.

Schutzhülle Eine Hülle oder ein Etui zum Schutz eines mobilen Geräts vor Beschädigungen.

Schwingspulenmotor Eine der beiden Methoden, den Positionierungsarm eines Festplattenlaufwerks zu bewegen. Siehe auch *Schrittmotor*.

SCSI (Small Computer System Interface) Eine langlebige Speicherlaufwerkstechnologie, die früher im Serverbereich gebräuchlich war. Es gab eine ganze Reihe Versionen. Heute lebt der SCSI-Befehlssatz in SAS-Laufwerken weiter. Siehe auch *SAS*.

SCSI-ID Eindeutige Kennung eines SCSI-Geräts. Zwei SCSI-Geräte dürfen nicht dieselbe ID verwenden.

SD (Secure Digital) Ein sehr verbreitetes Format von Flash-Speicherkarten, das auch Ein-/Ausgabegeräte unterstützt.

SDK (Software Development Kit) Software, mit der eigene Anwendungen für mobile Geräte entwickelt werden können.

SDRAM (Synchronous DRAM) Synchrones DRAM, das in Abhängigkeit vom Systemtakt regelmäßig aufgefrischt wird. Dieser RAM-Typ kommt in allen modernen Systemen zum Einsatz.

Secure Boot Ein UEFI-Feature, das einen sicheren Start gewährleisten soll, indem es korrekt signierte Software erforderlich macht. Das umfasst sowohl die eigentliche Boot-Software als auch Software, die bestimmte wichtige Komponenten unterstützt.

Segment Die Verbindung zwischen einem Computer und einem Switch.

Sektor Ein Segment einer der konzentrischen Spuren, die bei der Lowlevel-Formatierung einer Festplatte erzeugt werden. Bei älteren Festplatten enthält ein Sektor 512 Byte an Daten; moderne Festplatten verwenden 4096 Byte große *Advanced-Format*-Sektoren (AF-Sektoren).

Selbsterdung Ein nicht gerade ideales Verfahren, um elektrostatische Ladungen loszuwerden, indem man ein Objekt aus Metall berührt, etwa ein Computergehäuse. Selbsterdung kann auch bedeuten, sich ins stille Kämmerlein zurückzuziehen und mit sich selbst ins Reine zu kommen.

Selbstumschaltendes Netzteil Ein Netzteil, das die anliegende Spannung automatisch erkennt und sich entsprechend anpasst.

Seitenfehler Geringfügiger Fehler bei der Speicheradressierung.

Seitenverhältnis Das Verhältnis von Bildschirmbreite zu Bildschirmhöhe. Ältere Fernseher besitzen ein Seitenverhältnis von 4:3, neuere eines von 16:9. Computerbildschirme weisen meist ein Seitenverhältnis von 16:9 oder 16:10 auf.

Serieller Anschluss Ein bei älteren PCs gebräuchlicher Anschluss, an den Eingabegeräte (wie Mäuse) oder Modems angeschlossen werden. Wird auch als *COM-Port* bezeichnet.

Server Ein Computer, der seine Ressourcen, wie Drucker und Dateien, über das Netzwerk für andere Computer freigibt. Zum Beispiel ein NFS-Server, der seine Speicherkapazität einem Arbeitsplatzrechner bereitstellt, der keine eigene Festplatte besitzt.

Service Pack Eine Zusammenstellung von Software-Patches, die vom Softwarehersteller gleichzeitig veröffentlicht werden.

Set-Top-Box Ein Gerät, das einen Fernseher um Smart-TV-Features erweitert, wie z.B. Internet-Streaming oder das Aufzeichnen von Fernsehsendungen.

`sfc` (System File Checker) Ein Kommandozeilenprogramm (`sfc.exe`), das die Windows-Systemdateien, -ordner und -pfade überprüft und repariert oder wiederherstellt.

SFTP (Secure FTP) Sichere Version des File Transfer Protocol (FTP). Siehe *FTP*.

Shared Memory Siehe *Gemeinsam genutzter Speicher*.

Shell Ein Tool, das Eingaben auf der Kommandozeile verarbeitet. Wird auch als Kommandozeileninterpreter bezeichnet.

Shunt Siehe *Jumper*.

`shutdown` Windows- und Linux-Befehl zum Herunterfahren des Computers.

Sicheres Kennwort Ein mindestens acht Zeichen langes Kennwort, das Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthält.

Sicherheit am Arbeitsplatz Schützen Sie sich vor Gefahren.

Sichern und Wiederherstellen Das Backup-Werkzeug in Windows 7. Es bietet zwei Optionen: das Erstellen eines Backups oder die Wiederherstellung einer vorhandenen Datensicherung.

Sicherungs- oder Wiederherstellungs-Assistent Ein älteres Backup-Programm, das es dem Benutzer erlaubt, Backups des Systems und Wiederherstellungspunkte zu erstellen.

Sichtverbindung Bei Richtfunkstrecken und Übertragungen via Infrarot sind direkte Sichtverbindungen zwischen den Geräten erforderlich.

SID (Security Identifier) Eindeutige ID eines PCs, die beim Klonen von Festplatten normalerweise geändert wird.

Signatur Codemuster von Schadsoftware, das Anti-Malware-Software und Antivirenprogramme zur Erkennung von Malware verwenden.

Signierter Treiber Ein für Windows entwickelter Treiber, der getestet wurde und dem Microsoft bescheinigt, dass er ordnungsgemäß funktioniert.

SIMM (Single In-line Memory Module) Eine Bauform von DRAM-Speichermodulen, die für gewöhnlich 30 oder 72 Pins besitzen.

Slotblech Ein Streifen aus Metall, der einen nicht verwendeten Steckplatz auf der Rückseite des PCs abdeckt und so dafür sorgt, dass die Luftzirkulation im Gehäuse richtig funktioniert.

S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) Ein in Festplattenlaufwerken integriertes Überwachungssystem, das Fehler und Betriebsbedingungen einer Festplatte beobachtet.

Smartcard Eine kreditkartengroße Plastikkarte mit einem Chip, die zur Identifizierung des Kartenbesitzers dient.

Smartphone Ein Mobiltelefon, das Dinge ermöglicht, für die früher ein richtiger Computer erforderlich war, z.B. im Internet surfen, Dokumente anzeigen oder Medien konsumieren.

Smart Watch Eine Armbanduhr, die einige Features eines Smartphones besitzt und mit diesem kommunizieren kann.

S/MIME (Secure/Multipurpose Internet Mail Extension) Eine Technologie, mit der die Einstellungen für digitale E-Mail-Signaturen und Kontakte eines firmenweiten Adressbuchs konfiguriert werden.

SMTP (Simple Mail Transport Protocol) Das zum Versand von E-Mail im Internet verwendete Standardprotokoll, das den TCP-Port 25 nutzt.

Snap-Ins Kleine Hilfsprogramme, die über die Microsoft Management Console (MMC) aufrufbar sind.

Snapshot Ein Feature der Virtualisierung, das es erlaubt, eine Momentaufnahme des Systems zu erstellen, indem eine exakte Kopie der virtuellen Maschine gespeichert wird.

SNMP (Simple Network Management Protocol) Eine Reihe von Standards zur Kommunikation mit über ein TCP/IP-Netzwerk verbundenen Geräten, wie z.B. Router, Hubs und Switches. SNMP verwendet die TCP-Ports 161 und 162.

Social Engineering Das Manipulieren von Personen mit Zugang zu einer Netzwerkumgebung, um von außen auf das Netzwerk zugreifen zu können.

SO-DIMM (Small-Outline DIMM) Speichermodule, die aufgrund ihrer geringen Größe insbesondere in tragbaren Computern eingesetzt werden.

Softpower Ein Merkmal von ATX-Mainboards, die per Software ein- und ausgeschaltet werden können. Ob Softpower verwendet wird, ist an den Zuleitungen zum Ein/Ausschalter erkennbar. Anstelle der dicken in AT-Systemen verwendeten Stromleitungen sind am ATX-Schalter lediglich zwei dünne Drähte angeschlossen, die zum Mainboard führen.

Software Programme, die dafür ausgelegt sind, bestimmte Aufgaben zu erledigen und auf Massenspeichergeräten gespeichert werden.

Software-Firewall Eine auf Servern oder Arbeitsplatzrechnern laufende Firewall, die als Software implementiert ist. Siehe *Firewall*.

Software-Token Ein Programm, das normalerweise auf einem Smartphone oder Laptop läuft und es ermöglicht, das Gerät bei der Anmeldung an einer sicheren Ressource als Authentifizierungsfaktor einzusetzen.

Soundkarte Eine Erweiterungskarte, die über angeschlossene Lautsprecher Töne ausgibt.

Southbridge Ein Teil älterer Mainboard-Chipsätze, der für die Ein- und Ausgaben der vielen an einen PC angeschlossenen Geräte zuständig ist.

Spaces Ein Feature von macOS, das die Verwendung mehrerer Schreibtische erlaubt.

Spam Unerwünschte E-Mails von Geschäftemachern und Betrügern, die einen Großteil des E-Mail-Datenverkehrs im Internet ausmachen.

SPD (Serial Presence Detect) Auf einem RAM-Chip gespeicherte Informationen, die über seine Geschwindigkeit, seine Kapazität und weitere Aspekte Auskunft geben.

S/PDIF (Sony/Philips Digital Interface Format) Ein digitaler Audioanschluss, der bei vielen Soundkarten zu finden ist. Über diesen Anschluss können 5.1/7.1-Lautsprechersysteme direkt mit dem Computer verbunden werden. Zum Anschließen kann ein Koaxialkabel oder ein optisches Kabel verwendet werden.

Spannungsschienen PC-Netzteile, bei denen die Stromversorgung über mehrere Spannungsschienen erfolgt, die jeweils eine eigene maximale Leistungsaufnahme besitzen und auch über einen unabhängigen Strombegrenzungsschutz verfügen.

Spannungsstabilisierung Gewährleistet, dass die zum Betrieb eines Computers verfügbare Wechselspannung möglichst genau dem Sollwert entspricht. Die meisten unterbrechungsfreien Stromversorgungen bieten eine Spannungsstabilisierung.

Speicher Bauteile oder Medien, die während der Programmausführung vorübergehend Daten und andere Programme speichern. Meistens ist damit der interne Speicher eines Computers gemeint, auf den Programmbefehle direkt zugreifen können. Die RAM-Speicherkapazität wird in Kilobyte (KB), Megabyte (MB) oder Gigabyte (GB) angegeben. Die Speicherkapazität dauerhafter Speichermedien wie Festplatten oder SSDs bemisst sich ebenfalls in Megabyte, Gigabyte oder sogar Terabyte.

Speicheradressierung Die Speicheradressen des System-RAMs verweisen auf Speicherbereiche der Auslagerungsdatei oder auf ROM-Bereiche, die der CPU auf diese Wiese zugänglich sind.

Speicherbank Die Anzahl der DIMMs, auf die der Chipsatz gleichzeitig zugreifen kann. Sie ergibt sich, wenn man die Breite des externen Datenbusses durch diejenige des Datenbusses eines DIMMs teilt. Die DIMMs müssen sich in bestimmten Steckplätzen befinden, um den gleichzeitigen Zugriff zu ermöglichen.

Speicherplätze Eine Software-RAID-Lösung in Windows 8 und neueren Windows-Versionen, die mehrere Laufwerke zu einem einzigen Speicherpool zusammenfassen kann.

Sperrbildschirm Eine Sicherheitsfunktion von mobilen Geräten, die beim Einschalten des Geräts zum Entsperren die Eingabe eines Zahlencodes/Kennworts oder das Zeichnen eines Musters erfordert.

Spiegelung eines Volumes Das gleichzeitige Schreiben von Daten auf zwei (oder mehr) Laufwerke. Die Geschwindigkeit sinkt, aber die Redundanz wird erhöht.

Spoofing Gefälschte Informationen verwenden, um sich als jemand oder etwas anderes auszugeben. Gefälscht werden typischerweise MAC-, IP-, E-Mail- oder Web-Adressen oder Benutzernamen. Im Allgemeinen nützlich, um andere Angriffsmethoden wie Social Engineering oder Spear Phishing zu ergänzen.

Spotify (`spotify.com`) Ein Musikstreamingdienst.

Spreizen/Zusammenkneifen Eine Fingergeste, mit der Objekte vergrößert bzw. verkleinert werden können.

Sprites Rastergrafiken, z.B. BMP-Dateien, die von den ersten 3-D-Spielen zum Erzeugen einer dreidimensionalen Spielwelt verwendet wurden.

Sprungliste Ein seit Windows 7 verfügbares Menü, das kontextabhängige Informationen über Objekte in der Taskleiste anzeigt.

Spur Ein Bereich auf einer Scheibe eines Festplattenlaufwerks, der Daten speichert. Die auf mehreren Scheiben befindlichen Spuren gleichen Durchmessers werden als Zylinder bezeichnet.

Spyware Im Hintergrund laufende Software, die heimlich Informationen über die vom Benutzer besuchten Webseiten an den Hersteller der Spyware übermittelt.

SRAM (Static RAM) Ein RAM-Typ, der statt der bei DRAM üblichen Transistoren und Kondensatoren eine Flip-Flop-Schaltung zum Speichern von Informationen verwendet. SRAM muss nicht aufgefrischt werden und ist schneller als normales RAM. Wird vornehmlich für Cache-Speicher verwendet.

sRGB Standardisierter Farbraum, der dem Standard Dynamic Range (SDR) entspricht.

SSD (Solid-State-Drive) Ein Gerät, das zum Speichern von Daten einen Flash-Speicher verwendet.

SSH (Secure Shell) Ein Terminalemulationsprogramm, das Telnet ähnelt, mit dem Unterschied, dass alle Verbindungen verschlüsselt sind. SSH verwendet den TCP-Port 22.

SSID (Service Set Identifier) Ein Parameter, der ein drahtloses Netzwerk kennzeichnet; der Name des Netzwerks.

SSL (Secure Sockets Layer) Ein Verschlüsselungsprotokoll, das ein Browser für sichere Verbindungen zu einer Website verwendet.

Stammverzeichnis Das oberste Verzeichnis, das alle anderen Verzeichnisse enthält.

Standardbenutzerkonto Ein Benutzerkonto in Windows, das nur eingeschränkten Zugriff auf das System erlaubt. Diesem Kontentyp ist es nicht gestattet, Systemdateien zu modifizieren, Programme zu installieren oder über die Systemsteuerung Einstellung zu ändern, ohne ein Administratorkennwort anzugeben.

Standard Dynamic Range (SDR) 8-Bit-Farbstandard, der 256 Farben oder Graustufen definiert.

Standardgateway Der einem bestimmten Host nächste Router in einem TCP/IP-Netzwerk. Die IP-Adresse dieses Routers muss in den Einstellungen des Hosts konfiguriert sein, damit er mit anderen Netzwerken über IP kommunizieren kann.

Start Eine Schaltfläche in der Task-Leiste, die das Startmenü anzeigt.

Startbildschirm Die Windows-10-Version des Startmenüs, die eine Art Kombination aus dem herkömmlichen Startmenü und der Modern-UI-Benutzeroberfläche von Windows 8/8.1 darstellt.

Starthilfe Die erste Anlaufstelle zur automatischen Behebung einer Reihe von Problemen beim Systemstart.

Startmenü Ein Menü, auf das durch Anklicken der Schaltfläche START zugegriffen werden kann. Über das Startmenü können Sie alle auf dem System installierten Programme anzeigen und starten.

Statische IP-Adresse Eine fest zugewiesene IP-Adresse, die sich nicht ändert.

Stealth-Virus Ein Virus, das verschiedene Methoden verwendet, um nicht von einem Antivirenprogramm erkannt zu werden.

Steckbrücke Siehe *Jumper*.

Stecker Dienen dazu, Kabel an ein System anzuschließen. USB, PS/2, DB-25, RJ-45, HDMI, DVI, VGA, DisplayPort und Thunderbolt sind gebräuchliche Steckertypen.

Stereo Eine Audioaufnahme von zwei Quellen (Mikrofonen), im Gegensatz zu Monoaufnahmen, die nur eine Quelle verwenden.

Stern-Bus-Topologie Eine hybride Netzwerk-Topologie, bei der alle Computer an einem zentralen Bus – dem Switch – angeschlossen sind, die ansonsten jedoch die Merkmale einer Stern-Topologie aufweist.

Stern-Topologie Eine Netzwerk-Topologie, bei der alle Computer sternförmig mit einer zentralen Schaltstelle verbunden sind.

Stiftbedienung Eine von vielen PDAs verwendete Eingabemethode, die Handschriftenerkennung und Mausfunktionen bietet. Für gewöhnlich wird dazu ein Eingabestift benutzt, der einem Kugelschreiber ähnelt.

STP (Shielded Twisted Pair) Ein Netzwerkkabel, das aus abgeschirmten verdrillten Leitungspaaren besteht. Das Verdrillen dient dazu, Interferenzen zu reduzieren (das sogenannte »Übersprechen«) – je stärker die Kabel verdrillt sind, desto weniger Interferenzen entstehen. Die Leitungspaare werden durch eine metallische Abschirmung vor externen Interferenzen geschützt.

Strategie zur Fehlersuche Die Schritte zum Beheben eines Problems. Die CompTIA definiert sechs Schritte: Identifizieren des Problems; Aufstellen einer Theorie der wahrscheinlichsten Ursache; Über-

prüfen der Theorie; Erstellen eines Plans zur Problembehebung und dessen Umsetzung; Überprüfen, ob das System vollständig funktioniert; abschließend Befunde, getroffene Maßnahmen und Ergebnisse dokumentieren.

Stripesetvolumes Daten werden auf (mindestens) zwei verschiedene Volumes verteilt. Schreib- und Lesegeschwindigkeit werden dadurch erhöht. Entspricht einem RAID-0-Volume, da es keine Fehlertoleranz gibt.

Stripesetvolumes mit Parität Eine Methode um Fehlertoleranz zu erzielen. Dabei werden Paritätsdaten auf einem zusätzlichen Laufwerk gespeichert, die beim Ausfall einer Festplatte zur Datenrekonstruktion benutzt werden können. Für Disk Striping mit Parität werden mindestens drei Laufwerke benötigt: zwei für die Daten und ein drittes für die Paritätsdaten. Die RAID-Level 5, 10 und 0+1 verwenden Disk-Striping mit Parität mit verschiedenen Optionen, um Fehlertoleranz zu gewährleisten.

Strukturierte Verkabelung Ein ANSI/TIA-Standard, der den Aufbau einer Netzwerkverkabelung definiert, die einfach zu reparieren und leicht austauschbar ist.

`su` Älterer Linux-Befehl zum Erlangen von Root-Rechten.

Subnetzmaske Ein Wert für eine TCP/IP-Einstellung, der die IP-Adresse eines Hosts in eine Netzwerk-ID und eine Host-ID unterteilt.

Subpixel Die in LCD-Bildschirmen verwendeten, in Zeilen und Spalten zwischen polarisierenden Filtern ausgerichteten, winzigen Flüssigkristallmoleküle.

Subwoofer Ein kraftvoller Basslautsprecher, der Töne besonders niedriger Frequenz erzeugt.

`sudo` Linux-Befehl zum Erlangen von Root-Rechten.

Super-I/O-Chip Ein Chip, der speziell dafür ausgelegt ist, ältere und langsame Geräte wie Maus und Tastatur oder serielle und parallele Anschlüsse zu handhaben.

SuperSpeed-USB Ein USB-Standard mit einer Datenübertragungsrate von bis zu 5 Gbps, der auch als USB 3.0 bezeichnet wird.

SuperSpeed-USB+ Aktualisierte Version von SuperSpeed-USB mit einer Datenübertragungsrate von bis zu 10 Gbps, der auch als USB 3.1 bezeichnet wird.

SVGA (Super Video Graphics Array) Eine Bildschirmauflösung von 800 x 600. Bildschirme mit einer nativen Auflösung von 800 x 600 sind heutzutage eine Seltenheit, allerdings könnte Windows diesen Modus verwenden, wenn der Grafikkartentreiber defekt ist.

Swap-Datei Siehe *Auslagerungsdatei*.

Swap-Partition Eine spezielle Partition, die UNIX- und Linux-Systeme verwenden, die sich wie RAM verhält, wenn das System mehr Arbeitsspeicher als vorhanden benötigt.

Synchronisieren Der Vorgang, bei dem die auf Smartphone oder Tablet gespeicherten Daten und Dateien mit den auf dem Desktop-Computer oder den in der Cloud gespeicherten Daten abgeglichen werden.

Syntax Die korrekte Schreibweise eines Kommandozeilenbefehls, die eingehalten werden muss, damit er funktioniert und auch das bewirkt, was er erledigen soll.

`system/application log errors` Die Fehler und Warnmeldungen in diesem Protokoll können Hinweise auf das Vorhandensein einer Schadsoftware und deren Auswirkungen geben.

System-BIOS Das auf einem Flash-ROM auf dem Mainboard gespeicherte BIOS. Es stellt ein BIOS für die am Mainboard angeschlossene Hardware bereit, wie z.B. Tastatur-Controller, Grafikkarte und RAM.

Systembusgeschwindigkeit Die Geschwindigkeit, mit der die CPU und das übrige System arbeiten. Sie wird vom Systemquarz festgelegt.

Systemeinheit Der Hauptbestandteil eines PCs, der CPU, RAM, optische Laufwerke und Festplatten enthält. Die übrigen Geräte, wie Tastatur, Maus und Bildschirm, werden an der Systemeinheit angeschlossen.

Systemeinstellungen Ein Werkzeug in macOS, das zahlreiche Verwaltungsfunktionen bietet.

System File Checker Siehe *`sfc`*.

Systeminformationen Siehe *msinfo32*.

Systemkonfigurationsprogramm Siehe *msconfig*.

Systemlaufwerk Ein Speichergerät mit einem startfähigen Betriebssystem.

Systemmonitor Ein GNOME3-Werkzeug, das Systemressourcen wie CPU- und Arbeitsspeicherauslastung anzeigen und überwachen kann.

System on a Chip (SoC) Ein einzelner Chip, auf dem CPU, GPU und andere Schaltkreise vereint sind.

Systemquarz Ein Quarzoszillator, der den Takt für die CPU und das übrige System liefert.

Systemressourcen Kann durch die klassischen Begriffe Ein/Ausgabeadressen, IRQs, DMA-Kanäle und Speicheradressen beschrieben werden. Umfasst außerdem wesentliche Systemmerkmale wie Festplattenspeicherplatz, Menge des Arbeitsspeichers und die Prozessorgeschwindigkeit.

System-ROM Ein ROM-Chip, auf dem das BIOS gespeichert ist.

System-Setup-Utility Siehe *CMOS-Setup-Programm*.

Systemstartreparatur Siehe *Starthilfe*.

Systemsteuerung Eine Sammlung von Applets und kleinen Programmen, die dazu dienen, die Hardware und die Software eines Systems zu konfigurieren.

Systemwiederherstellung Ein Windows-Werkzeug, das es ermöglicht, eine bekanntermaßen funktionierende Konfiguration Ihres PCs wiederherzustellen, falls mal etwas schiefgeht. Bei der Systemwiederherstellung können Sie einen Wiederherstellungspunkt auswählen. Die Systemkonfiguration des Computers wird dann wieder in den Zustand versetzt, den sie beim Erstellen des Wiederherstellungspunkts besaß, ohne dass Ihre Daten oder E-Mails dabei in Mitleidenschaft gezogen werden.

%SystemRoot% Der Pfad des Verzeichnisses, in dem das Betriebssystem installiert ist.

T568A Ein Standard für die Pinbelegung von Ethernet-Steckern.

T568B Ein Standard für die Pinbelegung von Ethernet-Steckern.

Tablet Ein mobiles Gerät mit großem Touchscreen, das zum Surfen im Internet, zur Medienwiedergabe oder sogar zum Spielen verwendet werden kann.

Tablet-PC Ein kleiner tragbarer Computer, der sich von einem Tablet dadurch unterscheidet, dass er hauptsächlich mit einem Eingabestift bedient wird und Handschriftenerkennung verwendet.

Tägliches Backup Datensicherung aller Dateien, die an einem Tag geändert wurden, ohne das Archiv-Attribut zu verändern.

Tailgating Eine gängige Methode, um sich unerlaubten Zutritt zu erschleichen, indem man dicht hinter jemandem hergeht und mit ihm zusammen ein Gebäude betritt. Dabei tut man so, als ob man ganz selbstverständlich Zugang zu dem Gebäude hätte.

Taktfrequenz Die Geschwindigkeit, mit der eine CPU Befehle ausführt. Sie wird in MHz oder GHz angegeben. Bei modernen CPUs ist die interne Taktfrequenz ein Vielfaches des externen Systemtakts. Siehe *Taktvervielfachung*.

Taktleitung (CLK) Eine spezielle Leitung, an die ein Signal angelegt wird, das der CPU mitteilt, dass die nächsten Informationen zur Verarbeitung bereitstehen.

Taktvervielfachung Die CPU vervielfacht das externe Taktsignal, damit die internen Schaltkreise schneller arbeiten.

Taktzyklus Ein einzelnes an die Taktleitung der CPU angelegtes Signal.

Tap Siehe *Antippen*.

Task-Leiste Enthält die Schaltfläche START, den Infobereich, die Schnellstart-Symbolleiste und zeigt die laufenden Anwendungen an. Die Task-Leiste befindet sich standardmäßig am unteren Bildschirmrand.

`tasklist` Eine Kommandozeilenversion des Task-Managers.

Task-Manager Zeigt alle laufenden Programme, auch versteckte, und wird mit der Tastenkombination `Strg` + `⇧` + `ESC` aufgerufen. Sie können den Task-Manager zum sofortigen Beenden eines Programms verwenden, das sich auf normalem Wege nicht schließen lässt.

Tastatur Ein Eingabegerät, von dem es im Wesentlichen drei Typen gibt: Tastaturen mit USB- oder PS/2-Anschlüssen sowie drahtlose Tastaturen.

TCP/IP (Transmission Control Protocol/Internet Protocol) Ein vom US-amerikanischen Verteidigungsministerium entwickeltes Kommunikationsprotokoll, das es ungleichartigen Computern ermöglicht, über ein Netzwerk Informationen miteinander auszutauschen. TCP/IP ist das wichtigste Protokoll in fast allen modernen Netzwerken, auch im Internet.

TCP/IP-Dienste Dienste wie HTTP oder SSH, die über TCP/IP abgewickelt werden.

Telefonbetrug Eine Form des Social Engineerings, bei der ein Angreifer einen Mitarbeiter einer Organisation oder eines Unternehmens anruft, um an Informationen zu gelangen.

Telekommunikationsraum Der Raum, in dem die Leitungen zu den einzelnen Computern eines Netzwerks zusammenlaufen.

Telnet Ein Terminalemulationsprogramm für TCP/IP-Netzwerke, mit dem der Benutzer einen entfernten Rechner so bedienen kann, als ob er direkt vor ihm säße. Telnet verwendet den TCP-Port 23.

Tera Vorsilbe für 1.099.511.627.776 (2^{40}). Wenn es um die Speicherkapazität von Festplatten geht, ist damit meist 1 Billion Byte gemeint.

Terminal (1) Ein einfaches Endgerät, das mit einem Großrechner oder einem Computernetzwerk verbunden ist und zur Eingabe und Anzeige von Informationen verwendet wird.

Terminal (2) Ein Programm zur Eingabe von Kommandozeilenbefehlen in macOS und vielen Linux-Distributionen.

Terminalemulation Software, die sich wie ein bestimmtes Hardware-Terminal verhält und es einem Computer so ermöglicht, mit anderen Computern zu kommunizieren.

Tethering Die Verwendung eines mit einem Mobilfunknetz verbundenen mobilen Geräts als Hotspot.

Textur Eine kleine Grafik, mit der Wände, Böden und andere Oberflächen »gekachelt« werden, um eine 3-D-Welt zu erzeugen.

TFT (Thin Film Transistor) Ein Typ von LCD-Bildschirmen. Siehe *Aktiv-Matrix*.

Theorie der wahrscheinlichsten Ursache aufstellen Nach der Identifizierung des Problems hinterfragen Techniker das Offensichtliche, um die Ursache des Problems zu ermitteln. (Schritt 2 der CompTIA-Strategie zur Fehlersuche.)

Theorie überprüfen Versuchen Sie, ein Problem zu beheben, indem Sie die Theorie der Ursache bestätigen und in Erfahrung bringen, was zur Fehlerbehebung getan werden muss. Wenn sich die Theorie nicht bestätigt, müssen Sie eine neue entwickeln oder das Problem eskalieren. (Schritt 3 der CompTIA-Strategie zur Fehlersuche.)

Thermodrucker Ein Drucker, der einen beheizten Druckkopf verwendet, um hochwertige Bilder auf Normal- oder Spezialpapier auszugeben.

Thermopapier Ein spezielles wärmeempfindliches Papier für Thermodrucker.

Thick-Client Die CompTIA-Bezeichnung für einen normalen Desktop-PC. Auf diesen Computern läuft ein aktuelles Betriebssystem und sie können alle möglichen Anwendungen ausführen. Dieser PC-Typ sollte dem Großteil der Anforderungen von Leuten gerecht werden, die im Büro oder zu Hause einen Computer nutzen möchten. Ein Thick-Client benötigt keine Netzwerkverbindung und genügt den empfohlenen Systemanforderungen des Betriebssystems.

Thin-Client Ein System, das dafür ausgelegt ist, nur einfachste Anwendungen auszuführen, und lediglich die minimalen Hardware-Anforderungen des Betriebssystems erfüllt.

Thread Die kleinste logische Einheit, in die sich ein einzelnes Programm unterteilen lässt.

Thunderbolt Ein offener Standard für eine Schnittstelle, die vorwiegend zum Anschluss von Peripheriegeräten an Desktop-PCs oder Laptops verwendet wird, sofern diese über einen entsprechenden Anschluss verfügen.

Tier Die Unterteilung der verschiedenen Gruppen von Internetanbietern, die von den Tier-1-Providern mit eigenen Backbones bis zu Tier-3-Anbietern mit regionalen Netzwerken reicht.

Time Machine Das Werkzeug für vollständige Backups in macOS, das es ermöglicht, ausgewählte oder alle Dateien wiederherzustellen, falls eine Festplatte kaputtgeht. Time Machine gestattet es außerdem, versehentlich gelöschte Dateien oder ältere Dateiversionen wiederherzustellen.

Tintenpatrone Ein kleiner mit Tinte gefüllter Behälter für Tintenstrahldrucker.

Tintenstrahldrucker Ein Drucker, der mittels kleiner Düsen Tinte auf Papier sprüht, um Texte und Bilder auf Papier auszugeben.

TKIP (Temporal Key Integrity Protocol) Ein veralteter Verschlüsselungsstandard, der für jedes übermittelte Datenpaket einen neuen Schlüssel verwendet.

TN (Twisted Nematic) Eine ältere LCD-Technology. TN-Monitore liefern akzeptable Bilder und sind preiswert, besitzen aber einen geringen Blickwinkel und können nur einen beschränkten Farbraum darstellen.

Tonsonde Ein Gerät, das zusammen mit einem Tongenerator dazu verwendet wird, um das andere Ende eines Kabels aufzuspüren. Der Tongenerator erzeugt ein Signal bestimmter Frequenz, das an einem Ende des Kabels eingespeist wird. Erkennt die Tonsonde dieses Signal am anderen Ende des Kabels, gibt sie einen Ton von sich.

Toner Ein feines, aus an Eisenpartikel gebundenem Kunststoff bestehendes Pulver, das ein Laserdrucker dazu verwendet, Text und Grafiken zu Papier zu bringen.

Tonerkartusche Ein Behälter für den Toner eines Laserdruckers. Siehe auch *Laserdrucker* und *Toner*.

Topologie Die Art und Weise, auf der die Computer in einem Netzwerk miteinander verbunden sind.

Touch-Bedienung Die wichtigste Schnittstelle von Smartphones und Tablets, bei der die mechanische Tastatur durch berührungsempfindliche Bildschirme ersetzt ist.

Touchpad Ein flaches, berührungsempfindliches Feld, das bei den meisten Laptops als Zeigegerät Verwendung findet.

Touchscreen Ein Bildschirm, der die Position und die Dauer von Berührungen durch Finger oder einen Eingabestift erkennt.

`tracert` Kommandozeilenprogramm in Windows, das den Weg verfolgt, den ein Datenpaket nimmt, wenn es von einem Host zu einem anderen übertragen wird. In macOS und Linux heißt dieses Programm `traceroute`.

Trackball Ein Zeigegerät, bei dem mit den Fingern eine Kugel bewegt wird, um den Mauszeiger zu steuern.

TrackPoint Der von IBM entwickelte Joystick von der Größe eines Bleistiftradiergummis, der als Mausersatz für Laptops dient.

Transferrate Die Rate, mit der Daten zwischen zwei Geräten übertragen werden, insbesondere über den Erweiterungsbus.

Transport Layer Security (TLS) Ein Verschlüsselungsprotokoll, das für sichere Verbindungen zwischen Servern und Clients verwendet wird. Es kommt beispielsweise zum Einsatz, wenn sich Ihr Browser sicher mit Amazons Servern verbindet, wenn Sie einen Kauf tätigen. Ersetzt SSL.

Treibersignierung Eine digitale Signatur, die Windows dazu verwendet, das System vor potenziell schädlichen Treibern zu schützen.

Triple-Channel-Architektur Vergleichbar mit der Dual-Channel-Architektur, allerdings sind drei statt zwei RAM-Module erforderlich.

Trojanisches Pferd Ein Programm, das etwas anderes tut als das, was der Benutzer erwartet. Wird dazu verwendet, bösartigen Code zu verbergen.

Trusted Platform Module (TPM) Eine Hardware-Plattform zur Beschleunigung kryptografischer Funktionen und dem sicheren Speichern verschlüsselter Daten. BitLocker benötigt beispielsweise einen TPM-Chip auf dem Mainboard, um beim Booten überprüfen zu können, ob am Rechner Änderungen vorgenommen wurden.

Tunneln Eine verschlüsselte Verbindung zwischen auf zwei verschiedenen Computern laufenden Programmen herstellen.

TV-Empfänger Typischerweise ein externes Gerät, das den Empfang von Fernsehprogrammen ermöglicht.

TWAIN (Technology Without An Interesting Name) Eine Programmierschnittstelle, die es Grafikprogrammen wie Desktop-Publishing-Anwendungen ermöglicht, auf Scanner, Framegrabber oder andere bildaufzeichnende Geräte zuzugreifen.

UAC (User Account Control) Siehe *Benutzerkontensteuerung*.

UART (Universal Asynchronous Receiver/Transmitter) Ein Gerät, das parallele Daten in serielle wandelt und umgekehrt. Grundlage für die Verwendung serieller Anschlüsse und Modems.

Übergreifendes Volume Ein Volume, das Speicherplatz auf mehreren dynamischen Datenträgern verwendet.

Überspannungsschutz Ein preiswertes Gerät, das Ihren Computer vor Spannungsspitzen schützt.

Übertaktung Eine CPU oder GPU höher takten als vom Hersteller vorgesehen.

UDF (Universal Data Format) Ersetzte das ISO-9660-Format und ermöglicht es allen Betriebssystemen, mit einem optischen Laufwerk UDF-formatierte Medien zu lesen.

UEFI (Unified Extensible Firmware Interface) Eine moderne 32- oder 64-Bit-Schnittstelle zur Programmierung der Firmware. Hat das 16-Bit-BIOS ersetzt. UEFI unterstützt Laufwerke mit sehr großer Speicherkapazität und bietet weitere Features. Der Bootvorgang ist beispielsweise direkter.

Ultrabook Ein dünner, leistungsstarker Laptop mit Intel-Prozessor, der gemäß der Intel-Spezifikationen für Ultrabooks gefertigt ist und direkt mit Apples MacBook Air konkurrieren soll.

Unautorisierter Zugriff Der unerlaubte Zugriff auf Ressourcen, der sowohl unabsichtlich als auch in böser Absicht erfolgen kann.

Unbeaufsichtigte Installation Eine skriptgesteuerte Methode zur Installation des Betriebssystems, bei der kein Eingriff durch den Benutzer erforderlich ist.

UNC (Universal Naming Convention) Einheitliche Schreibweise des Netzwerkpfades gemeinsam genutzter Ressourcen gemäß der Konvention `\\<Servername>\<Name der Ressource>`.

Ungepuffertes RAM RAM-Bausteine ohne Puffer-Chip, also ganz normales RAM für Endkundengeräte.

Unicode Eine 16-Bit-Zeichencodierung, die alle Zeichen der häufigsten Sprachen sowie mehrere Tausend Symbole umfasst.

Unsignierter Treiber Ein Treiber, der das Windows Hardware Certification Program zur Gewährleistung der Kompatibilität nicht absolviert hat und daher von Microsoft nicht signiert wurde. Auf modernen Windows-Rechner sind sie nur noch selten anzutreffen, weil lediglich die letzten 32-Bit-Versionen von Windows unsignierte Treiber unterstützen.

Unterbrechung Das Anhalten eines Vorgangs, etwa die Ausführung eines Computerprogramms, auf eine Weise, die es gestattet, ihn nahtlos wieder fortzusetzen. Die Unterbrechung kann durch ein externes Ereignis ausgelöst werden, z.B durch Überwachungssensoren, oder durch einen Benutzer, der eine entsprechende Taste betätigt.

Unterer Koronadraht Ein dünner Draht, der von anderen Drähten geschützt wird, der das Papier positiv auflädt, damit die negativ geladenen Tonerpartikel während des Druckvorgangs von der Belichtungstrommel auf das Papier gezogen werden. Bei neueren Druckern wird derselbe Effekt durch eine Ladewalze erzielt, die den Toner von der Trommel aufs Papier befördert. Siehe auch *Koronadraht*.

Unterordner Ein Ordner, der sich in einem übergeordneten Ordner befindet.

UPC (Universal Product Code) Ein Barcode, der zur Überwachung von Lagerbeständen eingesetzt wird.

Upgrade-Installation Die Installation von Windows in den Ordnern einer bereits vorhandenen Windows-Installation, bei der die vorhergehenden Einstellungen für Hardware und Software übernommen werden.

UPS (Uninterruptible Power Supply) Siehe *USV (Unterbrechungsfreie Stromversorgung)*.

URL (Uniform Resource Locator) Eine Adresse, die den Speicherort einer Ressource im Internet angibt. URLs werden am häufigsten zusammen mit HTML und dem World Wide Web verwendet.

USB (Universal Serial Bus) Ein universeller serieller Anschluss für Tastaturen, Drucker, Joysticks und zahlreiche andere Geräte, der das Entfernen oder Anschließen von Geräten im laufenden Betrieb erlaubt.

USB-Host-Controller Ein Schaltkreis, der für gewöhnlich Teil des Chipsatzes ist und die an ihn angeschlossenen USB-Geräte steuert.

USB-Hub Ein Gerät, das einen einzelnen USB-Anschluss um zwei oder mehr USB-Anschlüsse erweitert.

USB-Root-Hub Derjenige Teil des Host-Controllers, der die physische Verbindung mit den USB-Anschlüssen herstellt.

USB-Speicherstick Ein Flash-Speichergerät, das den Standard-USB-Anschluss verwendet.

USB-Typ-C-Anschluss Ein verpolungsgeschützter Anschluss, der USB-SuperSpeed+ (USB 3.1) mit Datenübertragungsraten von bis zu 10 Gbps unterstützt. Er wird bei Android-Geräten schnell zu einem De-facto-Standard. Thunderbolt-fähige USB-Typ-C-Anschlüsse erreichen Datenübertragungsraten von bis zu 40 Gbps. Siehe auch *Thunderbolt*.

User Datagram Protocol (UDP) Verbindungsloses Protokoll, das TCP/IP verwendet. Siehe *TCP/IP*.

USMT (User State Migration Tool) Siehe *Migrationstool für den Benutzerstatus*.

USV (Unterbrechungsfreie Stromversorgung) Ein Gerät, das ein Computersystem kontinuierlich mit einer konstanten Spannung versorgt und es vor Stromausfällen und Spannungsspitzen oder -abfällen schützt.

UTP (Unshielded Twisted Pair) Ein weitverbreitetes Kabel für Telefonleitungen und Netzwerke, das aus verdrillten Leitungspaaren besteht. Das Verdrillen dient dazu, Interferenzen zu reduzieren (das sogenannte »Übersprechen«) – je stärker die Kabel verdrillt sind, desto weniger Interferenzen entstehen. Im Gegensatz zu STP-Kabeln gibt es bei UTP-Kabel keine metallische Abschirmung zum Schutz vor externen Interferenzen. UTP-Kabel werden in 1000BaseT-Netzwerken und vielen anderen Netzwerktypen verwendet. UTP-Kabel gibt es in vielen verschiedenen Qualitäten, die wie folgt in Kategorien (CAT) unterteilt sind:

CAT1	Standard-Telefonleitung; wird nicht für Datenübertragungen verwendet.
CAT2	Datenübertragungsraten von bis zu 4 Mbps
CAT3	Datenübertragungsraten von bis zu 16 Mbps
CAT4	Datenübertragungsraten von bis zu 20 Mbps
CAT5	Datenübertragungsraten von bis zu 100 Mbps
CAT5e	Datenübertragungsraten von bis zu 1000 Mbps
CAT6	Datenübertragungsraten von bis zu 10 Gbps
CAT6a	Datenübertragungsraten von bis zu 10 Gbps
CAT7	10-Gbps-Netzwerke (100 Meter lange Segmente); die Abschirmung einzelner Leitungspaare verringert das Übersprechen der Signale und dämpft das Rauschen. CAT7 ist *kein* ANSI/TIA-Standard.

Variablen Beim Programmieren oder der Skript-Erstellung werden Bezeichnungen für im Arbeitsspeicher abgelegte Daten verwendet. Ein Skript oder ein Programm kann die in einer Variablen gespeicherten Daten ändern oder ersetzen.

Verarbeitung Der zweite Schritt eines Rechenvorgangs, bei dem die CPU die Benutzereingaben verarbeitet.

Verbindliche Kommunikation Eine Form der Kommunikation, die weder aufdringlich noch bevormundend ist, aber auch nicht zu zurückhaltend. Sie ist nützlich im Umgang mit verärgerten Kunden, weil sie sowohl die Situation entschärft als auch zeigt, dass Sie wissen, was Sie tun.

Verbindungsstatusanzeige Eine LED, die konstant leuchtet, wenn die Verbindung mit einer Netzwerkkarte, einem Hub oder einem Switch ordnungsgemäß funktioniert.

Verbrauchsmaterial Das von Druckern verbrauchte Material, wie Papier, Tinte, Farbbänder und Tonerkartuschen.

Vererbung Ein NTFS-Feature, durch das neu angelegte Ordner oder Dateien dieselben Berechtigungen erhalten wie der übergeordnete Ordner.

Vermaschtes Netz Eine Netzwerk-Topologie, bei der die Endgeräte mit einem oder mehreren anderen Endgeräten verbunden sind. Diese Topologie kommt vornehmlich in drahtlosen Netzwerken zum Einsatz.

Verschlüsselung Das Umwandeln von Daten in eine Form, die nur lesbar ist, wenn das Kennwort oder der Schlüssel bekannt ist.

Verstärkungsverhältnis Ein Maß für die Signalverstärkung von Antennen, das in Dezibel (dB) angegeben wird.

Versteckt-Attribut Ein Dateiattribut, das die Anzeige einer Datei durch den `dir`-Befehl unterbindet.

Vertices Finden in der zweiten Generation der Berechnungsverfahren von 3-D-Grafiken Anwendung; die X-, Y- und Z-Koordinaten eines Vertex in der 3-D-Welt sind eindeutig definiert.

Vertikalfrequenz Siehe *Bildwiederholfrequenz*.

VESA-Halterung (Video Electronics Standards Association) Eine von der VESA standardisierte Befestigungsmöglichkeit, um ein Gerät beispielsweise an der Wand zu montieren oder an einem Ständer festzuschrauben, für die Größe, Position und Art festgelegt ist.

Verwahrungskette Der dokumentierte Verlauf des Besitzes eines bestimmten Geräts.

Verwaltung Eine Sammlung von Applets in der Systemsteuerung. Dazu gehören unter anderem Computerverwaltung, Ereignisanzeige und Leistungsüberwachung.

Verzeichnis Ein anderer Ausdruck für Ordner.

Verzeichnisdienst Ein zentralisiertes Verzeichnis, auf das alle PCs einer Domäne zugreifen können, um lokale Ressourcen zu finden.

VGA-Anschluss (Video Graphics Array) Ein 15-poliger, dreireihiger DB-Anschluss, der oft auch D-Sub-Anschluss oder eben VGA-Anschluss genannt wird. VGA ist der älteste und leistungsschwächste Monitoranschluss.

`vi` Kommandozeilenprogramm in Linux und macOS zum Bearbeiten von Textdateien.

Videoaufnahme Das Aufzeichnen von Videodaten wie Fernsehsendungen oder Spielfilme.

Virtual Machine Manager (VMM) Siehe *Hypervisor*.

Virtual Network Computing (VNC) Ein Protokoll, das Remotedesktop-Verbindungen ermöglicht. Siehe *Remotedesktop*.

Virtualisierte Arbeitsplatzrechner Ein Computer, auf dem mehrere virtuelle Maschinen laufen, stellt diese als Arbeitsplatzrechner bereit. Der Rechner muss leistungsfähig genug sein, um das normale Betriebssystem und die virtuellen Maschinen mit ihren Betriebssystemen ausführen zu können. In der Praxis ist dazu eine leistungsstarke 64-Bit-CPU mit mehreren Kernen und möglichst viel RAM erforderlich.

Virtuelle Maschine (VM) Eine vollständige Umgebung für ein Gastbetriebssystem, das so arbeitet, als ob es auf einem eigenständigen Computer installiert wäre.

Virtuelle Netzwerkkarte Eine Software-Netzwerkkarte einer VM, die die physische Netzwerkkarte des Wirtssystems nutzt, um auf das Netzwerk zuzugreifen, mit dem das Wirtssystem verbunden ist.

Virtuelle Realität Siehe *VR*.

Virtueller Assistent Sprachgesteuerte Software, die auf Benutzeranfragen antwortet und Informationen bereitstellt. Ein virtueller Assistent kann z.B. das Internet durchsuchen, Erinnerungen einrichten, Berechnungen durchführen oder Apps starten.

Virtueller Desktop Ein Desktop-Betriebssystem, das auf einer VM installiert ist. Ein lokales System kann eine eigene VM ausführen, auf der ein virtueller Desktop läuft, oder sich über das Netzwerk mit einem virtuellen Desktop verbinden, der auf einem Server läuft.

Virtueller Drucker Software, die sich als Drucker präsentiert, aber ein Dokument gar nicht unbedingt druckt, sondern in einem bestimmten Dateiformat (z.B. als PDF) speichert.

Virtueller Speicher Siehe *Auslagerungsdatei.*

Virtueller Switch Eine Software-Version eines Switches, die ein Hypervisor erzeugt, um virtuelle Maschinen miteinander zu vernetzen.

Virus Ein Virus ist ein Programm, das zwei Aufgaben erledigt: Replikation und Aktivierung. Bei der *Replikation* kopiert sich das Virus selbst. Bei der *Aktivierung* wird das Virus tätig und beschädigt das System oder löscht Dateien. Viren replizieren sich nicht direkt über das Netzwerk. Zur Verbreitung ist es erforderlich, dass der Benutzer etwas unternimmt (Programm öffnen, Laufwerke anschließen usw.). Siehe auch *Virendefinitionsdatei.*

Virendefinitionsdatei Eine Datei, die Informationen enthält, anhand derer die Schutzsoftware Viren erkennen und sie entfernen kann. Die Virendefinitionsdatei sollte möglichst oft aktualisiert werden. Manche Hersteller bezeichnen diese Datei auch als Virensignaturdatei.

Virenschild Passive Überwachung der Computeraktivität. Eine Virenüberprüfung findet nur bei Eintritt bestimmter Ereignisse statt.

VMM (Virtual Machine Manager) Siehe *Hypervisor.*

VoIP (Voice over Internet Protocol) Eine Sammlung verschiedener Protokolle, die Telefongespräche über Datenleitungen ermöglichen.

VoIP-Telefon Ein Gerät, das wie ein normales Telefon aussieht, aber zur Kommunikation über ein Computernetzwerk VoIP verwendet.

Vollduplex Gleichzeitiges Senden und Empfangen von Daten.

Vollständige Funktionalität überprüfen Vergewissern Sie sich, dass ein Problem wirklich behoben ist und nicht wieder auftreten kann. (Schritt 5 der CompTIA-Strategie zur Fehlersuche.)

Volt (V) Die Maßeinheit für die elektrische Spannung.

Volume Ein zusammenhängender Bereich von Zylindern oder Speicherblöcken auf einer Festplatte, der als eigenständige Speichereinheit behandelt wird.

Voucher Eine Möglichkeit, einen Preisnachlass für die CompTIA A+-Zertifizierungsprüfungen zu erhalten.

VPN (Virtual Private Network) Eine verschlüsselte Verbindung über das Internet zwischen einem Computer oder einem entfernten Netzwerk und einem privaten Netzwerk.

VR (Virtuelle Realität) Von einem Computer erzeugtes 3-D-Video und Audio, das eine virtuelle Welt simuliert, in der ein Benutzer navigieren kann (für gewöhnlich mithilfe von Bewegungssensoren und einem VR-Headset), indem er sich in der echten Welt bewegt.

VR-Headset Ein Headset oder eine Brille, die es dem Träger ermöglicht, mit der simulierten Welt zu interagieren. Siehe auch *VR.*

Waitstate Tritt ein, wenn die CPU darauf warten muss, dass der Arbeitsspeicher Code bereitstellt. Wird auch als *Pipeline-Stall* bezeichnet.

WAN (Wide Area Network) Eine geografisch weit verteilte Gruppe von Computern, die über Fernleitungen miteinander verbunden sind.

WAP (Wireless Access Point) Ein Gerät, das an zentraler Stelle drahtlose Netzwerkknoten miteinander verbindet.

Wärmeleitpaste Eine teigige Masse, die eine sehr hohe Wärmeleitfähigkeit besitzt. Sie wird zwischen CPU und Kühlkörper aufgebracht und gewährleistet, dass die von der CPU erzeugte Wärme möglichst gut abgeleitet wird.

Warteschlange Speichert Objekte, die auf ihre Verarbeitung warten. Ein Beispiel ist die Druckerwarteschlange, in der Druckaufträge darauf warten, abgearbeitet zu werden.

Wartezyklus Siehe *Waitstate*.

Wartungscenter Eine Zusammenfassung von Ereignissen, Warnhinweisen und Wartungsmeldungen in Windows 7 und neueren Windows-Versionen.

Wartungskit Ein aus verschiedenen Verbrauchsmaterialien und Verschleißteilen bestehendes Sortiment, das viele Hersteller für ihre Drucker anbieten.

WAV Ein Dateiformat für naturgetreue Audioaufnahmen, das PCM (Pulse Code Modulation) verwendet. Die so erzeugten Dateien sind sehr groß.

Webbrowser Ein Programm zum Abrufen, Interpretieren und Darstellen von Webseiten.

Webserver Ein Computer, der die Dateien speichert und bereitstellt, die eine Website bilden.

Webcam Eine PC-Kamera, die vor allem dazu verwendet wird, Videos über das Internet zu übertragen.

Wechseldatenträger Datenspeicher, die problemlos entfernt werden können, wie z.B. optische Medien, USB-Sticks oder Speicherkarten.

Wechselstrom Eine Form des elektrischen Stroms, bei dem die Flussrichtung periodisch wechselt (AC, *Alternating Current*).

WEP (Wireless Equivalent Privacy) Ein veraltetes Protokoll zur drahtlosen Datenübertragung, das ein 40-Bit-Verschlüsselungsverfahren verwendet. Es bietet keine vollständige Ende-zu-Ende-Verschlüsselung und ist angreifbar.

Werkzeugsatz Ein Techniker sollte immer einige unverzichtbare Werkzeuge dabeihaben. Dazu gehören etwa Kreuzschlitz- und Schlitzschraubendreher, eine Pinzette, eine Aderklemme, ein Torx-Schraubendreher, ein Federarmgreifer und ein paar Steckschlüssel für Innensechskantschrauben.

Widerstand (1) Ein Maß dafür, wie schwierig es ist, elektrischen Strom durch ein Material fließen zu lassen. Der elektrische Widerstand wird in Ohm angegeben.

Widerstand (2) Ein Bauteil, das dem Fließen eines elektrischen Stroms einen Widerstand entgegensetzt. Siehe auch *Ohm*.

Wiederherstellung Das Reparieren der durch ein Virus angerichteten Schäden.

Wiederherstellungspunkt Eine mit dem Wiederherstellungs-Werkzeug erstellte Momentaufnahme, die zur Reparatur eines nicht mehr ordnungsgemäß funktionierenden Systems verwendet werden kann. Siehe auch *Systemwiederherstellung*.

Wi-Fi Siehe *WLAN*.

Wi-Fi Protected Setup (WPS) Ein von vielen WAPs und Clients eingesetzter Standard, der die Konfiguration sicherer Verbindungen erleichtert. Allerdings sollte WPS deaktiviert werden, weil es eine große Sicherheitslücke aufweist.

Wildcard Ein Zeichen – für gewöhnlich ein Stern (*) oder ein Fragezeichen (?) – zur Festlegung von Suchkriterien. Beispielsweise liefert die Suche nach `*.docx` als Ergebnis eine Liste aller Dateien mit der Erweiterung `.docx`. Bei dieser Suche ist * die Wildcard. Wildcards können in Kommandozeilenbefehlen benutzt werden, um Befehle auf mehrere Dateien gleichzeitig anzuwenden.

Windows 7 Eine Windows-Version, von der verschiedene Editionen für die Nutzung zu Hause oder im Büro verfügbar sind, die es jedoch nicht als Serverversion gibt. Wurde von Windows 8/8.1 abgelöst.

Windows 8/8.1 Eine Windows-Version, die durch die neue Modern-UI-Bedienoberfläche hervorsticht. Es gibt Versionen für Desktop-PCs, Laptops, Smartphones und Tablets. Wurde von Windows 10 abgelöst.

Windows 10 Eine Windows-Version, die heute auf den meisten Desktops und Laptops läuft.

Windows EasyTransfer Ein Werkzeug für Windows 7/8/8.1, um Dateien und Einstellungen auf einen anderen PC zu übertragen. In Windows 10 ist es nicht verfügbar.

Windows-Explorer Ein Programm zum Durchstöbern der auf den Laufwerken eines PCs gespeicherten Ordner und Dateien.

Windows Hardware Certification Program Das strenge Testprogramm für Hardware-Hersteller, das deren Geräte durchlaufen müssen, damit Microsoft die Gerätetreiber digital signiert.

Windows PowerShell Das in Windows enthaltene Kommandozeilenwerkzeug, das eine Vielzahl leistungsfähiger Skripting-Tools zur Automatisierung von Änderungen sowohl lokal als auch im Netzwerk bietet.

Windows-Speicherdiagnosetool Ein seit Windows 7 verfügbares Werkzeug, das automatisch das RAM eines Computers überprüfen kann, falls es Probleme bereitet.

Windows-Taste Die Taste mit dem Windows-Logo öffnet traditionellerweise das Startmenü, findet aber auch bei einigen Tastaturkürzeln Verwendung.

Windows-Vorinstallationsumgebung (WinPE) Das Windows-Installationsprogramm.

Windows-Wiederherstellungsumgebung Eine Reihe von Werkzeugen im Windows-Setup, die verschiedene Möglichkeiten zur Fehlerbehebung und Reparatur bieten.

Windows-Sidebar Ein Feature von Windows Vista, das es dem Benutzer erlaubt, am rechten Rand des Desktops Minianwendungen zu platzieren, z.B. Uhr, Kalender oder andere Hilfsprogramme.

Windows Update Microsofts Programm, das Windows-Betriebssysteme auf dem neuesten Stand hält und Patches oder Verbesserungen einspielt. Siehe auch *Automatische Updates*.

WinPE (Windows Preinstallation Environment) Siehe *Windows-Vorinstallationsumgebung*.

WinRE (Windows Recovery Environment) Siehe *Windows-Wiederherstellungsumgebung*.

Windows Vista Eine Windows-Version, von der verschiedene Editionen für die Nutzung zu Hause oder im Büro verfügbar sind, die es jedoch nicht als Serverversion gibt.

Windows XP Eine Windows-Version, die Windows 2000 und sämtliche Windows-9x-Versionen abgelöst hat, von der es keine Serverversion gibt. Windows XP wird seit April 2014 von Microsoft nicht mehr unterstützt. Wurde von Windows Vista abgelöst.

Windows-XP-Modus Eine vorgefertigte virtuelle Maschine mit Windows XP Service Pack 3, die zusammen mit den Professional-, Ultimate- und Enterprise-Editionen von Windows 7 ausgeliefert wird. Sie ermöglicht die Ausführung von älteren Programmen, die mit Windows 7 nicht kompatibel sind.

Wischen Eine Geste zur Bedienung von mobilen Geräten, bei der Sie den Bildschirm mit einem Finger berühren und diesen dann nach oben oder unten bzw. nach rechts oder links bewegen, je nach Art der Anwendung.

Wischgestenentsperrung Eine Feature von mobilen Geräten, das es ermöglicht, ein Gerät durch das Zeichnen eines Musters zu entsperren.

Wissensdatenbank Eine von Microsoft gepflegte umfangreiche Sammlung von Dokumenten und häufig gestellten Fragen. Sie ist auf der Website von Microsoft zu finden und eine ausgezeichnete Anlaufstelle, um nach Hilfe zu suchen, wenn Schwierigkeiten mit dem Betriebssystem auftreten.

WLAN Drahtloses Netzwerk nach dem Standard IEEE 802.11.

WLAN-Telefonie Ein Feature von mobilen Geräten, das es erlaubt, Telefongespräche statt über ein Mobilfunknetz per WLAN zu führen.

Workgroup Ein einfaches, dezentrales Netzwerk, das Windows-PCs standardmäßig verwenden.

WPA (Wi-Fi Protected Access) Ein Protokoll zur drahtlosen Datenübertragung, das zur Verschlüsselung TKIP/EAP verwendet und die Schwachstellen von WEP beheben soll. Wurde inzwischen durch WPA2 abgelöst.

WPA2 (Wi-Fi Protected Access 2) Ein Protokoll zur drahtlosen Datenübertragung, für das auch die Bezeichnung IEEE 802.11i geläufig ist. Es verwendet zur Verschlüsselung AES und ersetzt WPA.

Wrapper Siehe *Containerdatei*.

Wurm Ein spezielles Virus, das im Gegensatz zu normalen Viren keine anderen Dateien auf einem Computer infiziert. Stattdessen erstellt es auf *anderen* Systemen im Netzwerk Kopien seiner selbst, indem es sich Sicherheitsschwachstellen in Netzwerkprotokollen zunutze macht.

WUXGA Eine Bildschirmauflösung von 1.920 x 1.200.

WWW (World Wide Web) Ein System von Internetservern, die HTML-Dateien und Dateien in verwandten Formaten bereitstellen. Der Zugriff darauf erfolgt mittels Anwendungen, die HTTP oder HTTPS verwenden, wie z.B. Webbrowser.

`www.comptia.org` Website der CompTIA.

WXGA Eine Bildschirmauflösung von 1.280 x 800.

x64 Kennzeichnet 64-Bit-Betriebssysteme und 64-Bit-Software.

x86 Kennzeichnet 32-Bit-Betriebssysteme und 32-Bit-Software.

`xcopy` Ein Kommandozeilenprogramm, das im Gegensatz zum normalen `copy`-Befehl mehrere Verzeichnisse auf einen Schlag kopieren kann.

xD-Karte (Extreme Digital Picture Card) Ein sehr kleines Flash-Speicherkartenformat.

Xeon Eine Modellreihe von Intel-Serverprozessoren.

XGA (Extended Graphics Array) Eine Bildschirmauflösung von 1.024 x 768.

XPS-Druckpfad (XML Paper Specification Print Path) Ein Drucksystem in Windows, das ein verbessertes Farbmanagement und erweiterte Layoutmöglichkeiten bietet.

Yagi Yagi-Antennen mit mehreren Elementen sind Richtantennen, die den Empfang lediglich in einer bestimmten Richtung verbessern. Sie ähneln den Hausantennen, die früher zum Empfang von Fernsehprogrammen verwendet wurden, sind allerdings deutlich kleiner.

Zeitpunkt für das Ausschalten auswählen In den Energieoptionen können Sie einstellen, wann der Bildschirm abgeschaltet oder der Computer in den Ruhezustand versetzt wird und so Ihren eigenen Energiesparplan einrichten.

Zero-day-Angriff Ein Angriff, der einen zuvor unbekannten Bug oder eine noch nicht bekannte Schwachstelle ausnutzt. Die Bezeichnung geht darauf zurück, dass die Entwickler der Hardware oder der Software genau null Tage Zeit hatten, das Problem zu beheben.

Zertifizierung Ein Beleg für Kompetenz in einem bestimmten Fachbereich.

ZIF-Sockel (Zero Insertion Force Socket) Ein Prozessorsockel, bei dem zum Einsetzen der CPU keinerlei Kraft erforderlich ist. Die CPU gleitet sanft an Ort und Stelle und wird dann mit einem kleinen Hebel arretiert.

Zigbee Ein komplett offenes drahtloses Netzwerkprotokoll, das für die Hausautomation gedacht ist.

Zombie Ein mit Schadsoftware infizierter Computer, der dadurch zum Bestandteil eines Botnetzes geworden ist.

Zweikern-Prozessor Eine CPU mit zwei Prozessorkernen auf einem Chip, die sich Cache- und Arbeitsspeicher teilen.

Zwischenfallbericht Dokumentieren Sie die Einzelheiten von Zwischenfällen, vor allem was genau geschehen ist und wo sich ein Vorfall zugetragen hat.

Z-Wave Ein proprietäres Protokoll für drahtlose Netzwerke (mit einer offenen API für Programmierer), das für die Hausautomation gedacht ist.

Stichwortverzeichnis

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

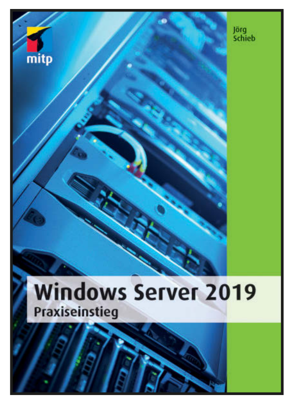
W

X

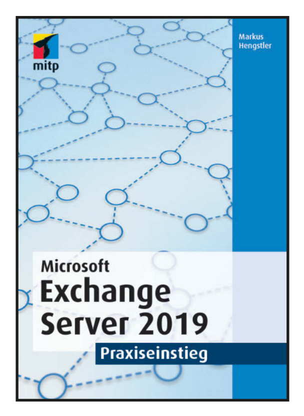
Y

Z

Systemadministration

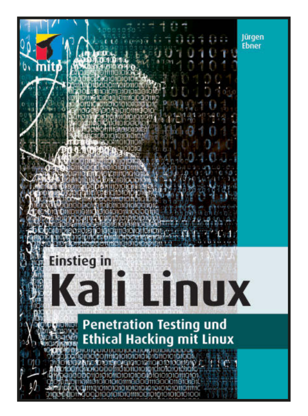


ISBN 978-3-95845-887-1

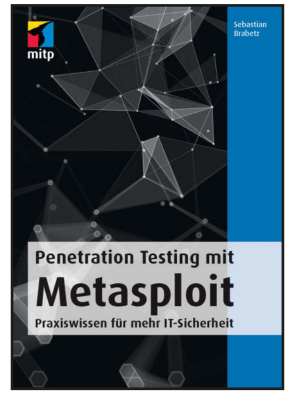


ISBN 978-3-95845-745-4

IT-Sicherheit



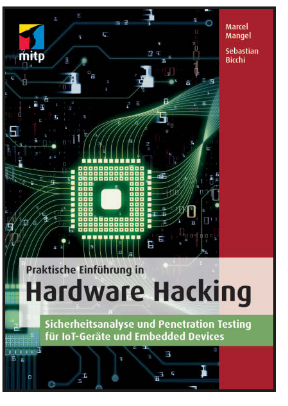
ISBN 978-3-7475-0033-0



ISBN 978-3-95845-595-5



ISBN 978-3-95845-968-7



ISBN 978-3-95845-816-1